BLOG DI EXODUS1984

Tecnologia, informatica, natura, e l'intero universo.... :-)

BLOG

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License.

Questo breve libro elettronico è stato creato per raccogliere i post del mio blog in questa prima versione, perchè molte persone volevano avere un blog “offline” da poter consultare e per ricercare articoli senza una connessione ad internet. :-)

Approfitto di questa occasione per ringraziare I gestori del provider LIBERO.IT che mi hanno permesso di creare e mantenere questo blog.

Versione 1.0.0 2013

blog parte 1

@Enrico De Cecco 1984-2013

messaggio di benvenuto per tutti gli utenti di questo blog

Post n°1 pubblicato il **06 Marzo 2012** da exodus1984
Un saluto particolare a tutti i componenti e i lettori di questo nuovo blog.

Presto potro' postare dei nuovi articoli che penso possano essere molto utili a tutti.

Gli amici del pinguino... :-)

Post n°2 pubblicato il **18 Marzo 2012** da exodus1984
Iniziamo con qualche pillola semplice semplice.

Per i problemi di connessione 3G, su Linux ci sono diverse metodologie per ottenere un buon livello di segnale, elenchiamo i piu' semplici:

1) key 3G con prolunga usb ATTIVA

2) router 3G con rj45 e wifi disponibili

3) amplificazione della key 3G

Se siete utenti in mobilita', allora non dovreste avere grossi problemi di connessione, ma se siete utenti fissi e senza una linea DSL, allora le cose si complicano per tutti voi, ma possiamo risolverle in modo adeguato.

Molte persone comprano un router 3G e poi dividono la connessione in casa con i vari computer, questo e' un buon inizio.

ricordatevi solo di installare il router 3G in posizione elevata(possibile soffitta...) in modo da guadagnare molto segnale HSPA/UMTS e diffondere il segnale wi-fi altrettanto bene all'interno del vostro stabile.

Esistono router 3G che operano con sistemi Linux ed offrono un'ottima configurazione utente come protezione DDOS, Firewall SPI, URL...

Per oggi e' tutto, continueremo le descrizioni tecniche nella prossima puntata. ;-))

Un saluto ai visitatori di questo blog e buona navigazione a tutti

Analisi delle key... 8-P

Post n°3 pubblicato il **26 Marzo 2012** da exodus1984
Buonasera a tutti voi cari blogger, stasera perleremo delle chiavette internet, ovvero gioie e dolori(+dolori...) di una connessione internet mobile... :-))

Qualcuno di voi avra' certamente smontato una di queste chiavette che sono tanto di moda oggigiorno, e quindi passiamo al sodo: taroccamento e spippolamento finale per ottenere una buona connessione anche in aree non proprio coperte dal servizio.

Le chiavette internet sono davvero utili se siamo in mobilita' e non abbiamo altre fonti di connessione valide per raggiungere internet, ma le particolarita' tecniche costruttive, ne determinano l'utilizzo corretto per tutti i nostri scopi.

Con opportune modifiche, so puo' adattare una parabola satellitare al supporto della chiavetta per ottenere un buon rapporto di segnale sia ricevuto che trasmesso.

A questo punto si dovra' puntare la parabola verso una cella conosciuta(posizione verticale) e guardando il livello di segnale ricevuto sul programma di connessione, si potra' determinare il corretto puntamento verso il sistema emettitore principale.

Dovete notare che la cella a seconda del carico dati, potrebbe mandare la vostra chiavetta a fare visita ad un'altra emittente, percui se volete lavorare bene da postazioni fisse, vi conviene fare la posizione della cella telefonica piu' vicina alla vostra abitazione e quindi puntarla per bene.

Le key usano un sistema di connessione particolare come quello per i cellulari, infatti, e' la cella telefonica che comanda la vostra key internet, dicendogli dove deve andare....(AFFAAAN...) ;-)))

La prossima volta vedremo come ottenere un segnale ottimo in modo che sia la vostra key a dire alla cella emittente dove deve andare....(vedi sopra...) per ottenere un'ottima tenuta di banda in scaricamento anche se siete moolto lontani dalla vostra cella preferita...(lasciate ogni speranza voi che entrate...in rete).

Per oggi e' tutto cari bloggers, ci leggiamo alla prossima puntata e di nuovo, buona navigazione a tutti voi :-)

una settimana davvero avvincente!!!

Post n°4 pubblicato il **29 Aprile 2012** da exodus1984

Buonasera cari bloggers, dal ritorno in rete dopo un po' di tempo in giro a smanettare sulle reti, vi saluto tutti cordialmente, e naturalmente auguro a tutti voi sempre le solite vecchie cose, ovvero una buona navigazione in internet e felici spippolamenti di rete .... ;-))))

Allora, per incominciare, stasera vi racconto di un vecchio signore che non sapeva cosa fosse l'insalata, questo signore provo' un grande piacere a seminare l'orto e a raccogliere l'insalata da lui seminata che ritrovo' la voglia di creare e di ripartire con una nuova vita.

Che cosa ci insegna tutto questo? Ci insegna che abbiamo sempre bisogno di imparare qualcosa di nuovo, la nostra sete di conoscenza deve essere colmata sempre in tutti i modi possibili ed impossibili.

Carissimi bloggers, nella vita bisogna sempre dare agli altri tutto cio' che si ritiene opportuno in un determinato momento della vostra vita reale e virtuale, ma non dimenticate che la conoscenza e' potere, e questo potere va' usato con saggezza.

Tutti noi abbiamo dei pregi e dei difetti visibili ed invisibili, ma siamo sempre unici nel nostro genere e l'unicita' del nostro essere virtuale, fa' si' che possiamo creare e fare cose assolutamente uniche che molti poi potranno invidiarci per molto, moltissimo tempo a venire.

Il nostro mondo e' la rete, la nostra realta' virtuale nella quale ci specchiamo ogni giorno e ci confrontiamo con il resto del mondo, l'universo appartiene alle persone che lo sanno acchiappare senza essere legate ad alcun dettame filosofico, governativo, o di natura diversa dal nostro intelletto di rete.

Anche per stasera e' tutto cari bloggers, spero che le poche righe che oggi vi ho mandato, possano servirvi per capire e trovare la vostra strada nel mondo virtuale in cui viviamo.

A tutti, un grande saluto e buona navigazione, ci leggiamo alle prossime puntate de: "Gli amici del Pinguino" :-)

Analisi forensi di livello informatico

Post n°5 pubblicato il **01 Maggio 2012** da exodus1984
Cari bloggers, oggi impariamo ad usare uno dei comandi piu' importanti di un sistema, ovvero quello che dice agli altri cosa avete fatto, come lo avete fatto e quando.... ;-))

E' il caso di spiegare che il comando touch puo' creare e manipolare i file del vostro sistema, ma chi di voi e' preparato, sapra' benissimo cosa si puo' fare e cosa NON si dovrebbe fare con questo comando.... :-))
Noi analizzeremo cosa NON si dovrebbe fare con questo comando:

Il comando touch puo' manipolare ogni tipo di file sul vostro sistema, e puo' forzare altri comandi come il make e il comando find a vedere solo quello che voi gli direte che puo' essere visto, ovvero controllate cio' che gli altri vedranno sul vostro sistema, e a questo punto, avrete il pieno controllo delle persone che cercano di controllare voi e i vostri file(la classica parabola dei Pifferi di Montagna, che vennero per suonare e finirono suonati) .... :-))

Carissimi bloggers, immaginate per un solo istante di potervi inserire nella mente di un pirata informatico, che cosa penserebbe? Penserebbe appunto di modificare le tracce della sua permanenza sui sistemi degli altri, anche se' non si puo' dire esattamente cosi'... ;-)

Analizziamo quindi in breve come creare alibi elettronici per i file di sistema, prendiamo un file che potrebbe essere compromettente per voi e non volete che chi controllera' i vostri documenti possa riferirlo a voi come prova, quindi lo modificate e vi costruite sopra la storia dell'orso che non aveva soldi per riscaldarsi in inverno e fu' costretto a vendere la propria pelle per potersi comprare la legna con cui avrebbe acceso il fuoco... ;-)

Se appunto, avete fatto i tapiri su qualche server e avete conservato i trofei di rete nel vostro file preferito, questo file, non potrebbe piu' appartenere a voi, vediamo come:

Questo comando modifica la data di ultimo accesso al file tapirux:
touch -a -d '13 dec 1901 ' tapirux

Questo comando modifica la data dell'ultima modifica effettuata sul file tapirux:
touch -d '31 dec 2037 23:59:59' tapirux

La cosa interessante e' che ci sono di mezzo ben 136 anni in cui si possono creare alibi informatici e modificare prove elettroniche.

Le date sono molto interessanti: 13 dec 1901 22:59:59 e 31 dec 2037 23:59:59.
Dalle prove effettuate, non si possono creare file con date antecedenti al 1901 e postcedenti al 2037, anche gli orari sono statici: 22:59:59 per il 1901 e 23:59:59 per il 2037.
Naturalmente, su sistemi diversi le cose possono variare, quindi vi consiglio di testare fino a dove potete spingervi senza farvi troppo male...

Naturalmente questo documento e' inteso come strumento tecnico e non come istigazione a delinquere, la conoscenza deve essere libera e disponibile a tutti, percio' fatene buon uso e usatela con saggezza.

Di nuovo, buona navigazione a tutti voi, e non spippolate troppo la grande rete.... ;-))

Analisi del funzionamento di un calcolatore: il programma SimCpu per capire ed apprendere

Post n°6 pubblicato il **03 Maggio 2012** da exodus1984
Salve a tutti carissimi bloggers, questa sera analizzeremo come compilare
SimCpu su sistemi GNU/Linux e creare eseguibili anche per sistemi windows.

Per maggiori info, vi rimando direttamente al link del suo autore, dove potrete scaricarlo e dove potrete anche trovare tutta la documentazione che puo' servirvi per apprendere le basi del funzionamento di un calcolatore a basso livello.

Potete linkare SimCpu a questo indirizzo:

http://web.diegm.uniud.it/pierluca/public_html/teaching/fpac/strumenti/simcpu/doc/quick_start_web_it.html

E adesso passiamo al sodo...:-)

1 Compilazione da Linux per creare SimCpu su windows.
2 Compilazione su Debian Squeeze 2011 dell'assemblatore SimCpu.

Procedura da seguire su sistemi Debian con installazione di Mingw32.
Dopo avere installato Mingw32, sul proprio sistema abbiamo a disposizione
il nuovo tipo di compilatore:

```
i586-mingw32msvc-g++
```

##########################
Portarsi sotto la directory SimCpu e digitare il seguente comando per compilare l'eseguibile da usare solo su sistemi win32:

```
i586-mingw32msvc-g++ -target -mwin32 assembler.c -o assembler.exe
```

Viene creato l'eseguibile per sistemi Windows a 32 bit.

##########################

Per testarlo su Linux, usare Wine, aprire un terminale e digitare:

parsec@exodus84:~$ wine assembler.exe e quindi premere INVIO.

##########################

Compilare include.c per windows da Linux:

i586-mingw32msvc-g++ -mwin32 include.c -o include.exe

##########################

Per compilare l'eseguibile monolitico trasportabile su altri
sistemi linux che contiene gia' tutte le librerie che gli
servono per funzionare:

gcc --static assembler.c -o assembler

##########################

Per compilare l'eseguibile da usare solo per il nostro
sistema con librerie a caricamento dinamico:

gcc assembler.c -o assembler

##########################
Carissimi bloggers anche per questa sera e' tutto, buon divertimento
e come sempre, buona navigazione a tutti voi :-)

Utility portatili, BusyBox: il "coltellino svizzero" dei sistemi operativi

Post n°7 pubblicato il **04 Maggio 2012** da exodus1984
Salve a tutti cari bloggers, oggi ci occupiamo di uno strumento unico e affidabile che serve per creare micro-distribuzioni Linux, che puo' essere usato per violare sistemi o recuperare sistemi in difficolta'.

BusyBox e' definito il coltellino svizzero dei sistemi operativi perche' puo' effettuare operazioni amministrative dove non si riesce a recuperare
o riorganizzare un sistema operativo compromesso dall'uso che gli utenti ne' fanno oppure da sistemi hardware compromessi.

Il link dove potete scaricare l'ultima versione stabile e' questo:

http://www.busybox.net/

Allora proseguiamo:

Dopo che avrete scaricato l'ultima versione considerata stabile dovete
aprire l'archivio .tar.bz2 nella sua directory di creazione:

busybox-1.19.4

a questo punto ci portiamo sotto la directory busybox-1.19.4
e da terminale diamo il comando:

make menuconfig confermando l'esecuzione con il tasto Invio.

Ora siamo sull'interfaccia di BusyBox e possiamo decidere quali strumenti
dovremo portarci dietro dopo che avremo compilato il nostro eseguibile di sistema in modalita' statica, ovvero se volete portarvi dietro il vostro coltellino svizzero informatico, questa e' la modalita' che vi serve se non volete avere problemi con le librerie a caricamento dinamico su sistemi Linux
differenti dal vostro sistema di compilazione originale.

Per sapere se il vostro nuovo eseguibile e' affidabile, ovvero viene creato un grosso file del peso di circa 2 mega (+ o -), anche qui usiamo un classico
terminale e digitiamo il seguente comando:

ldd busybox confermando l'esecuzione sempre con il tasto Invio.

not a dynamic executable

Se il comando ldd vi fornisce questa risposta, allora potete caricare il vostro nuovo coltellino svizzero su una chiavetta usb, quindi attaccarla alle chiavi dell'auto per essere sempre pronti ad ogni evento informatico spiacevole sia per voi che per i vostri sistemi operativi... ;-))

Fatto questo, testiamo subito il nostro nuovo strumento, sotto la directory di compilazione di busybox-1.19.4 da terminale diamo il seguente comando:

parsec@exodus84:~/busybox-1.19.4$ ./busybox

BusyBox v1.19.4 (2012-05-04 21:29:49 CEST) multi-call binary.
Copyright (C) 1998-2011 Erik Andersen, Rob Landley, Denys Vlasenko
and others. Licensed under GPLv2.
See source distribution for full notice.

Usage: busybox [function] [arguments]...
  or: busybox --list[-full]
  or: function [arguments]...

   BusyBox is a multi-call binary that combines many common Unix
   utilities into a single executable. Most people will create a
   link to busybox for each function they wish to use and BusyBox
   will act like whatever it was invoked as.

   [, [[, acpid, add-shell, addgroup, adduser, adjtimex, ar, arp, arping, ash, awk, base64, basename, beep,

blkid, blockdev, bootchartd, brctl, bunzip2, bzcat, bzip2, cal, cat, catv, chat, chattr, chgrp, chmod, chown, chpasswd,
chpst, chroot, chrt, chvt, cksum, clear, cmp, comm, cp, cpio, crond, crontab, cryptpw, cttyhack, cut, date, dc, dd, deallocvt, delgroup, deluser, depmod, devmem, df, dhcprelay, diff, dirname, dmesg, dnsd, dnsdomainname,
dos2unix, dpkg, dpkg-deb, du, dumpkmap, dumpleases, echo, ed, egrep, eject, env, envdir, envuidgid, ether-wake, expand, expr, fakeidentd, false, fbset, fbsplash, fdflush, fdformat, fdisk, fgconsole, fgrep, find, findfs, flock,
fold, free, freeramdisk, fsck, fsck.minix, fsync, ftpd, ftpget, ftpput, fuser, getopt, getty, grep, groups, gunzip, gzip, halt, hd, hdparm, head, hexdump, hostid, hostname, httpd, hush, hwclock, id, ifconfig, ifdown, ifenslave,
ifplugd, ifup, inetd, init, insmod, install, ionice, iostat, ip, ipaddr, ipcalc, ipcrm, ipcs, iplink, iproute, iprule, iptunnel, kbd_mode, kill, killall, killall5, klogd, last, less, linux32, linux64, linuxrc, ln, loadfont,
loadkmap, logger, login, logname, logread, losetup, lpd, lpq, lpr, ls, lsattr, lsmod, lspci, lsusb, lzcat, lzma, lzop, lzopcat, makedevs, makemime, man, md5sum, mdev, mesg, microcom, mkdir, mkdosfs, mke2fs, mkfifo, mkfs.ext2,
mkfs.minix, mkfs.vfat, mknod, mkpasswd, mkswap, mktemp, modinfo, modprobe, more, mount, mountpoint, mpstat, mt, mv, nameif, nbd-client, nc, netstat, nice, nmeter, nohup, nslookup, ntpd, od, openvt, passwd, patch, pgrep, pidof,
ping, ping6, pipe_progress, pivot_root, pkill, pmap, popmaildir, poweroff, powertop, printenv, printf, ps, pscan, pstree, pwd, pwdx, raidautorun, rdate, rdev, readahead, readlink, readprofile, realpath, reboot, reformime,
remove-shell, renice, reset, resize, rev, rm, rmdir, rmmod, route, rpm, rpm2cpio, rtcwake, run-parts, runlevel, runsv, runsvdir, rx, script, scriptreplay, sed, sendmail, seq, setarch, setconsole, setfont, setkeycodes,
setlogcons, setserial, setsid, setuidgid, sh, sha1sum, sha256sum, sha512sum, showkey, slattach, sleep, smemcap, softlimit, sort, split, start-stop-daemon, stat, strings, stty, su, sulogin, sum, sv, svlogd, swapoff, swapon,
switch_root, sync, sysctl, syslogd, tac, tail, tar, tcpsvd, tee, telnet, telnetd, test, tftp, tftpd, time, timeout, top, touch, tr, traceroute, traceroute6, true, tty, ttysize, tunctl, ubiattach, ubidetach, ubimkvol, ubirmvol,
ubirsvol, ubiupdatevol, udhcpc, udhcpd, udpsvd, umount, uname, uncompress, unexpand, uniq, unix2dos, unlzma, unlzop, unxz, unzip, uptime, users, usleep, uudecode, uuencode, vconfig, vi, vlock, volname, wall, watch, watchdog, wc,
wget, which, who, whoami, whois, xargs, xz, xzcat, yes, zcat, zcip

Come potete vedere, questa carrellata di comandi puo' gestire quasi tutte le emergenze che potrebbero affliggere la vostra LinuXBoX preferita.
Carissimi bloggers, se avete compilato bene il vostro eseguibile, avrete a disposizione uno strumento di grandissimo valore informatico sempre pronto ad affrontare le sfide di sopravvivenza di rete che al giorno d'oggi, ci piacciono davvero tanto... ;-)

Buona navigazione a tutti voi e buon divertimento informatico con il vostro nuovo giocattolo... 8-P

Essere anonimi in rete: il sistema operativo Tails

Post n°8 pubblicato il **06 Maggio 2012** da exodus1984
Carissimi bloggers, salve a tutti voi, oggi parleremo dell'anonimato in rete, che cosa può offrirci e come possiamo usare al meglio questo servizio.

Per prima cosa, analizzeremo uno dei sistemi operativi Linux più conosciuti per effettuare tunnel e salti "anonimi" da un punto all'altro della grande rete internet.
Per iniziare subito a comprendere le funzionalità di una connessione "anonima" vi mando subito a visitare questo indirizzo web, dove potrete scaricarvi una copia di questo sistema operativo basato su Debian 6.0.4 .

https://tails.boum.org/

Detto questo passiamo ad analizzare la distribuzione di Tails, questo sistema operativo e' completo di tutto quello che serve per mantenere la propria privacy, ma fate attenzione, ricordo a tutti voi che la vera sicurezza in rete, non esiste, al riguardo anche la distribuzione di Tails non e' del tutto esente da questa banale considerazione.

Molti buchi di sistema sono stati chiusi ma con il test della distribuzione, ne' saranno scoperti moltissimi altri, per cui il consiglio che vi posso dare e' quello di non affidarvi SOLO al sistema operativo per la vostra sicurezza, ma anche a comportamenti corretti che dovrebbero essere sempre tenuti in rete, su ogni rete esistente, appunto perché in rete ci sono persone molto diverse e sempre pronte a rubare la fiducia della gente e con la fiducia della gente, poi si possono fare cose davvero distruttive per chi come noi, vive e convive sulla grande rete... :-9

Nelle versioni precedenti di Tails, alcuni buchi sulla sicurezza di rete, permettevano agli spammers di rintracciare un indirizzo e-mail usato da un utente che aveva in esecuzione questo sistema per fargli ritrovare poi nella propria casella e-mail un sacco di messaggi indesiderati... :-U
Una rapida occhiata agli indirizzi IP dei messaggi, riportavano appunto alle connessioni usate e loggate quando il sistema era in esecuzione temporanea su supporto DVD.

Connessioni internet di Tails:
##############################
A parte i buchi sulla sicurezza, di cui ogni sistema operativo ha il proprio fardello da portarsi dietro, il sistema Tails permette di avere anche una veloce connessione mobile e quindi può essere usato con (quasi)tutte le chiavette internet a disposizione dei principali sette(7) operatori di telefonia mobile italiani:

3
CoopVoce
Fastweb
PosteMobile
TIM
Vodafone
Wind

Questa particolare configurazione, viene effettuata conoscendo il proprio operatore mobile, indicando un eventuale operatore non inserito in elenco e le modalità di connessione usate(GSM, GPRS, EDGE, UMTS,HSPA, CDMA/1xRTT, EVDO) dalla rete indicata indicando se possibile il piano tariffario e concludendo con l'applicazione delle modifiche effettuate per avere accesso alla propria connessione internet.

Servizi offerti da Tails:
##############################
Tails sfrutta la rete Tor, implementando tunnel cifrati che nascondono di fatto sia un semplice client che intere strutture server, và da se che se un server implementato su una rete Tor puo' offrire di conseguenza servizi anonimi e criptati come siti web, ftp, ssh(servizi cifrati su rete cifrata).

Accesso ROOT di Tails:
##############################

Nell'ultima versione di Tails, l'accesso root e' stato negato per motivi di sicurezza, per cui quando avviate il sistema da DVD, alla schermata di login può essere attribuita una password che sarà utilizzata dall'utente per accedere ai servizi amministrativi come synaptic per aggiornare le Key usb, ricordate che se al primo login non immettete una password qualsiasi, dopo essere entrati sull'account non avrete la possibilità di accedere a servizi con privilegi più alti, se non avete impostato una password il comando dato da terminale: "sudo su" vi riporterà un errore critico negandovi qualsiasi accesso superiore al sistema.

Installazione di Tails su USB:
##############################
Vediamo ora come creare una key usb usando questo sistema dopo il boot da DVD.
Quando avrete configurato tutto quello che vi serve sulla distribuzione live di Tails, e' giunto il momento di inserire una chiave usb e procedere con le utility fornite a corredo del menu' principale, verrà aperto un programma dove potrete scegliere quale tipo di installazione volete avere su key usb, ovvero creazione e installazione da immagine live, aggiornamento e upgrade
oppure una partizione cifrata dove depositare il sistema configurato e pronto per il prossimo avvio, con tanto di password per aprire la key criptata all'avvio.
Bisogna ricordare che se si abilita una persistenza dei dati su chiave usb, questo potrebbe compromettere la sicurezza personale in quanto il sistema salva programmi e configurazioni in modo fisso(apt-get,key pgp,nodi visitati, etc...), mentre se si salva solo una copia di Tails su chiave usb, bisognerà ripetere le configurazioni preliminari ad ogni avvio del sistema, ma questo è un modo molto più sicuro per l'uso di questo sistema operativo.

Rimasterizzazione di Tails su DVD:
##############################
Per ri-masterizzare una copia di Tails con le vostre modifiche e aggiungendo
programmi personali, dovrete procedere in questo modo:
Caricate una copia dell'iso di Tails su una directory di lavoro sotto la vostra HomeDirectory, quindi aggiungete i programmi che ritenete utili durante le vostre navigazioni "anonime" e ricreate un nuovo file .iso che poi provvederete a depositare su un classico supporto CD/DVD.
Per mantenervi ad un livello di sicurezza adeguato, vi consiglio di non modificare lo squash-FS originale di Tails, perchè come abbiamo accennato in precedenza, la persistenza dei vostri dati potrebbe pregiudicare la sicurezza finale ottenuta in questo modo.
Vediamo ora come procedere:

Creiamo una directory "anonym2011", dove depositeremo i files estratti dall'iso originale di Tails:

/home/parsec/anonym2011

Quando avrete apportato tutte le vostre modifiche, potete procedere alla creazione di un nuovo file .iso bootabile, da terminale potete ricreare il vostro file iso digitando i seguenti comandi:

genisoimage -V "AnoX2011" -copyright cpr.txt -p anox2011 -publisher anox2011 -J -R -o anox2011.iso -b isolinux/isolinux.bin -c isolinux/boot.cat -no-emul-boot -boot-load-size 4 -boot-info-table /home/parsec/anonym2011

++++++++++++++++++++++++++++

Alla fine del processo di ricostruzione, avremo il nostro nuovo sistema
operativo modificato di nome : anox2011.iso .

Testiamo adesso il nostro lavoro appena terminato, prima di creare fisicamente il DVD, perchè se quello che avete appena creato non vi soddisfa, potete cambiarlo tutte le volte che volete, senza buttare via nessun supporto CD/DVD :

emulazione iso file:

qemu -m 2047 -smp 8 -cdrom anox2011.iso

Se disponete di un pc con poca memoria ram e processori obsoleti, eliminate
dalla riga di comando di Qemu i parametri -m e -smp, l'emulatore scegliera' i parametri in base al sistema che avete a disposizione, e questo potrebbe richiedere anche molto tempo prima di poter vedere il vostro nuovo sistema operativo "anonimo" in azione... ;-))
Per cui, se le vostre nuove modifiche vi sembrano adeguate, allora procedete con la masterizzazione del vostro file.iso su supporto fisso CD/DVD.

A questo punto, cari bloggers, potete provare il sistema, per la keyusb e il dvdlive dovrete accedere al programma sul bios del vostro computer, indicando il supporto hardware che volete usare come boot prioritario, ovvero
il boot da cd/dvd oppure da key usb (hdd).

Molto bene, anche per oggi abbiamo terminato e come sempre, auguro una buona navigazione a tutti voi e felici ricerche (quasi) anonime sulla grande rete... ;-))

Chiavette internet: impariamo a migliorarne le prestazioni

Post n°9 pubblicato il **08 Maggio 2012** da exodus1984
Carissimi bloggers, oggi parleremo di come si può aumentare fisicamente il segnale delle chiavette internet.
Ho scritto questo semplice articolo per colmare alcuni vuoti "tecnologici" che gli utenti alle prime armi, ma anche utenti con un livello avanzato potrebbero avere nel costruire un impianto di rete "fissa" basato esclusivamente sull'uso di connessioni mobili.

Durante le numerose installazioni che ho fatto, ho riscontrato numerosi problemi relativi al basso segnale ricevuto, al calore emesso dalle chiavette internet, ai luoghi dove le suddette installazioni dovevano essere fatte.
Ebbene, oggi impareremo a costruire una connessione di rete mobile perche' possa essere usata agevolmente in casa, ovvero per tutte quelle persone che non dispongono di una connessione aXDSL su normale linea telefonica, perche' la banda larga non arriva ancora o non arrivera' mai nei loro comuni di residenza.

Prendiamo in considerazione le chiavette internet che vengono vendute oggigiorno, ci sono posti dove il segnale non arriva oppure ci si puo' connettere, ma la navigazione internet e' cosi' lenta che vi fa' rimpiangere davvero il vostro vecchio e caro modem a 57K... ;-))

Allora, come ovviare a questi problemi? Se qualcuno di voi ha smontato almeno una volta una di queste chiavette internet, allora avra' capito anche il perche' di tanti problemi, il primo problema e' che le chiavette si riscaldano parecchio specialmente quando la cella dell'operatore e' a distanza notevole da dove avete intenzione di connettervi, e quindi la cella stessa richiede alla vostra key di emettere piu' potenza in trasmissione, questo fatto pero', porta all'eccessivo surriscaldamento del modulo interno, diminuendone di fatto le prestazioni.

Iniziamo a risolvere questo problema, durante le varie installazioni che ho fatto, tutti i clienti si lamentavano appunto di questi due(2) problemi, da una rapida ispezione dei locali in cui il cliente avrebbe voluto avere una connessione affidabile, il segnale era sempre minimo e la navigazione internet cosi' lenta che anche leggere la posta elettronica era una vera e propria sfida. ;-)
Ho risolto questo problema semplicemente installando un router 3G, uno dei miei preferiti perche' gestito da un sistema GNU/Linux, vi ricordate di BusyBox il coltellino svizzero dei sistemi operativi?
Il modello interessato per chi di voi volesse provarlo e aumentare le prestazioni della propria chiavetta internet, e' questo:

AirLive Air3GII.

Questo modello di router 3G oltre che avere il supporto a 400+ tipi di chiavette internet diverse, puo' gestire anche una doppia connessione axDSL/3G/4G in modo che possiate avere sempre una possibilita' di essere connessi alla rete e quindi di poter lavorare.
Un consiglio se vi connettete con smartphone Apple S4:
dopo che avrete applicato le modifiche al router, riavviate il tutto e potrete navigare con il vostro 4S in wi-fi comodamente su una rete instradata da uno stabile sistema operativo basato su GNU/Linux .

Altre caratteristiche tecniche, potete trovarle sul sito del produttore, ma
ne' elenco alcune per farvi capire di cosa si tratta:

##############

Auto-Failover, ovvero quando non avete pagato la bolletta del telefono, e la vostra axDSL casalinga non funziona, entra in scena la connessione 3G/4G.

##############

Il controllo della connessione, ovvero potete lasciare attaccata la vostra chiavetta al router acceso, e vi connetterete solo digitando un indirizzo nella barra di navigazione del Browser, questa funzione bypassa il programma di connessione, ed e' utile perche' e' il router che accende e spegne la vostra connessione internet, quindi non avete bisogno di installare nessun programma sul pc.

##############

Su questo router, abbiamo il sistema di filtraggio avanzato, il controllo di connessioni wi-fi e il controllo MAC avanzato, inoltre disponiamo di una protezione attiva per il DDoS di rete(utile per sistemi windows).

##############

La configurazione via Browser, rende le cose molto semplici anche per utenti che non sono preparati a gestire un rete casalinga.

E con questo, cari bloggers anche per oggi e' tutto, la prossima volta parleremo di come poter sostituire la nostra chiavetta con qualcosa di piu' performante e tecnologico, per catturare ancora piu' segnale dalla BTS piu' vicina a noi, e quindi aumentare di brutto la nostra velocita' in scaricamento.

Di nuovo, a tutti voi, buona navigazione e ci ri-leggiamo alla prossima puntata de "Gli amici del Pinguino" ;-)))

Chiavette internet: il modulo Traveler3GM

Post n°10 pubblicato il **09 Maggio 2012** da exodus1984
Carissimi bloggers, eccoci qui per una nuova ed entusiasmante lezione di tecnologie di connessione internet.

La volta scorsa, abbiamo parlato del router wi-fi AirLive3gII, un ottimo prodotto, considerando il prezzo molto conveniente rispetto a tutte le funzioni avanzate che ci mette a disposizione per creare, connettere, controllare la nostra connessione internet (prezzo indicativo sui 40 Euro).

Per cui, come promesso, oggi parleremo degli effetti benefici che possiamo ottenere cambiando e sostituendo la nostra chiavetta internet, togliendo la nostra scheda Sim e inserendola di fatto in un nuovo tipo di modulo che ci permette di avere una ricezione del segnale BTS ancora maggiore, considerando appunto il sistema ricevente di una normale chiavetta internet.
Se volete provare questo modulo, potete cercarlo su internet o visitare il sito del distributore, il suo prezzo pero', si aggira sui 150 Euro, una spesa non indifferente per molte tasche al giorno d'oggi, ma giustificata dal fatto che il suddetto modulo, ci fa' navigare anche dove abbiamo pochissimo segnale utile, e che quindi merita di essere usato:

Traveler3GM AirLive

Personalmente, ho eseguito molte installazioni 3G usando questo modulo, e risolvendo di fatto il problema del segnale debole, infatti, molti clienti hanno potuto provarlo rimanendo molto soddisfatti, e quindi hanno deciso di acquistarlo, nonostante il prezzo elevato, tuttavia ci sono state comunque situazioni in cui il carico di rete mobile portava la connessione a essere veloce come una lumaca, e quindi in questi casi ho optato per il solo router
AirLive3gII, che usando la chiavetta originale e una sottorete wi-fi, dava migliori prestazioni.

Il sistema di cui parleremo oggi, e' un'implementazione tra un router wi-fi 3G/4G e una chiavetta internet di livello avanzato che monta un sistema GNU/Linux per la gestione completa delle connessioni di rete internet.

Il Traveler3GM della ormai nota AirLive, e' un ottimo sostituto delle chiavette internet che vengono vendute con sim inclusa.
Cio' che dovremo fare, e' alquanto semplice, dobbiamo estrarre la nostra scheda Sim dalla chiavetta che ci e' stata fornita all'attivazione della connessione internet ed inserirla nello slot predisposto sotto la batteria agli ioni di litio del modulo Traveler3GM.

Ricezione 3GM :
################
La ricezione e la trasmissione risultano subito molto piu' veloci e fluide della nostra normale chiavetta internet, questo perche' il Traveler3GM dispone di un modulo UMTS/HSPA/HSUPA molto innovativo che quindi gli permette di ricevere un segnale molto piu' pulito e forte di una normale internet key.

Accesso al modulo:
###################
Dopo avere caricato la batteria e inserito la vostra Sim, dovrete spostare verso il basso il pulsante che trovate sul modulo 3G appena sopra al cavo di alimentazione/connessione USB.
Un consiglio che vi posso dare e' che il primo setup di questo modulo andrebbe fatto su rete wi-fi appunto per testare le impostazioni di fabbrica e iniziare cosi' la vostra personale configurazione basandovi sul vostro operatore mobile, infatti il Traveler3GM supporta (quasi) tutti gli operatori mobili sparsi ai 4 angoli del pianeta, e per ogni operatore in ogni parte del mondo, ci sono i settaggi gia' predisposti se volete usarlo durante il vostro giro del mondo... ;-))

Settaggi preliminari:
######################
Al vostro primo setup, attivate il modulo wi-fi e attendete alcuni secondi affinche' il sistema si carichi e il server dhcpd vi fornisca un indirizzo
IP con il quale connettere la sottorete casalinga.

I parametri di configurazione sono questi:

indirizo IP del router 3G: 192.168.1.1
il nome login di default: admin
la password di default : airlive
l' SSID del router wi-fi : airlive

Naturalmente, per la vostra sicurezza, provvederete a cambiare gli indirizzi del router e la password, poi dovrete impostare il MAC e abilitare il filtraggio delle connessioni, decidendo come e quando un utente potra' connettersi al vostro router, e di conseguenza, navigare su internet.

Per i sistemi Windows, disponiamo di un ottimo supporto CDrom contenente i driver di installazione, le guide in formato PDF(in inglese), mentre e' compatibile e supportato da tutte le distribuzioni GNU/Linux via driver >option1>, e quindi non necessita di nessuna installazione di programmi come avviene per i sistemi Windows.
Per connettervi ad internet con questo modem/router3G, dovrete creare una connessione usando la applet NetworkManager che e' indicata sulla barra del menu del desktop Linux con due pc sovrapposti, i sistemi Linux moderni, hanno gia' tutti gli operatori mobili settati, dovrete solo scegliere il vostro e il tipo di piano tariffario che avete.

Sicurezza Traveler3GM:
##########################
Le funzioni di sicurezza del modem, sono molto avanzate e basate su un sistema GNU/Linux molto stabile, siccome ci sono moltissime funzioni utili, ne' citero' alcune tra le piu' semplici:

filtri IP, DDoS protection, host DMZ, setup UPnP(per sistemi Windows), filtri di dominio, blocco di URL, MAC control... ;-)

Noterete che una "semplice" chiavetta internet, non vi fornira' mai tutte queste funzioni di protezione, e che come conseguenza logica, con una normale chiavetta internet, vi beccate tutta la spazzatura che vi arriva dalla rete, mentre con dispositivi di questo tipo, avrete la capacita' di fermare in entrata tutto cio' che volete, mantenendo pulita, veloce e (abbastanza) sicura la vostra nuova rete casalinga, in questo modo, anche i vostri PC vi ringrazieranno, potrete implementare altri firewall e antivirus in cascata su ogni PC che avete a disposizione se volete aumentare la vostra sicurezza interna.

Nelle installazioni che ho fatto, ho visto chiavette internet a 14.4,28.8 viaggiare ai livelli inferiori a quelli di un buon 57K, gli operatori di rete mobile, si fanno la guerra a colpi di Megabit, ma chi ne' paga le conseguenze, e' sempre l'utente finale che si fida troppo delle loro promesse, e che non effetua un test di connessione preliminare dalla zona di residenza, acquistando un prodotto che sbandiera velocita' elevatissime anche dove non c'e' campo... ;-)

Per questo motivo, invito tutti voi a testare questi prodotti prima di comprarli, avendo trovato molti utenti insoddisfatti del prodotto appena acquistato.
Nella mia personale esperienza tecnica con il Traveler3GM, ho scaricato DVD a velocita' anche superiori a quelle indicate nelle specifiche della Sim(7.9,8.0 Mb/s), ma questa, e' un'altra storia.... ;-)))

Cari bloggers, riflettete bene prima di comprare una connessione mobile, verificate sempre la copertura e gli operatori disponibili, inoltre, il segnale ricevuto, puo' essere diverso usando diverse Sim di operatori diversi nella stessa zona, questo e' un metodo per sapere quale conessione conviene avere, anche se alcuni operatori fanno pagare di meno, prima valutate bene e pensateci sempre due o tre volte prima di prendere una scheda Sim di un determinato operatore mobile.

Anche per oggi e' tutto carissimi bloggers, spero che questo articolo possa essere utile a tutti voi, e possa aiutarvi ad avere la connessione internet che vi serve senza spendere troppi soldi.
Di nuovo, un saluto a tutti voi, e buona navigazione sulla grande rete :-)

Chiavette internet: i ripetitori UMTS

Post n°11 pubblicato il **10 Maggio 2012** da exodus1984
Carissimi bloggers, oggi terminiamo le nostre considerazioni al riguardo delle connessioni mobili, per cui dopo aver trattato la sostituzione delle nostre chiavette internet con il nuovo modulo Traveler3GM e aver creato una rete casalinga su connessione mobile con il router AirLive3gII, ora impareremo come potenziare al 100% il segnale BTS ottenendo di fatto una connessione piu' veloce sia per la navigazione che per lo scaricamento dati.

Parleremo di come installare ed usare i ripetitori di segnale UMTS, per ottenere una stabile e veloce connessione internet.
I ripetitori di segnale, sono un vero toccasana per chi deve lavorare su internet usando una connessione mobile, specialmente dove il segnale BTS e' fuggitivo o del tutto assente.

Iniziamo a vedere i componenti di queste particolari tecnologie elettroniche, avrete a disposizione il modulo ripetitore completo di due(2) antenne esterne, una dovra' essere puntata sulla BTS piu' vicina a voi o al vostro stabile, se siete in montagna, dovrete puntare l'antenna esterna verso il basso, con polarizzazione verticale(controllate sempre...) considerando la vostra altezza sul livello del mare.

Le antenne esterne, dovranno essere puntate verso una BTS predefinita, in quanto se ottenete un segnale valido e comunque la vostra connessione va' e viene, vorra' dire che le vostre antenne non sono puntate perfettamente e che quindi il modulo ripetitore, acchiappa 2 o 3 BTS dislocate nello stesso raggio di distribuzione, generando cosi' il cosiddetto effetto ping-pong che puo' sovraccaricare il ripetitore facendolo riavviare piu' volte, questo e' il motivo di un segnale che sembra ottimo, ma un attimo dopo non c'e' piu', infatti l'uso delle frequenze pilota delle varie BTS, si sovrappone generando questo effetto, che in molti casi dove le installazioni vengono fatte da utenti inesperti e non consapevoli, pregiudicano il risultato finale che e' quello di ottenere un segnale al 100% sia in entrata che in uscita.

Se volete provarne qualcuno, vi posso consigliare gli AnyTone, ma' ne' potete trovare di altre marche diverse.
Quello che posso dirvi sui repeater UMTS, e' che risolvono un grave problema delle reti mobili italiane, il segnale non arriva dappertutto oppure arriva male o e' addirittura inesistente, alcuni operatori di rete mobile, stanno fornendo ai loro clienti dei ripetitori da installare nella propria abitazione, ma non tutti lo fanno, per la classica legge di mercato:

"Ti vendo una key ad alta velocita', ma non ti garantisco la velocita'... eppoi, se vai piano, consumi il tuo credito subito, e alla fine non avrai ottenuto nulla..." ;-)))

Cari bloggers, gli operatori di rete mobile, non vi dicono tutto cio' che vi serve per avere una buona tenuta di banda con la vostra nuova key internet.
Negli anni in cui facevo assistenze informatiche di questo tipo, ho visto migliaia di clienti arrabbiati con il proprio operatore mobile solo perche' le chiavette internet venivano pubblicizzate a 7.2 Mb/s e i clienti le compravano subito perche' poi avrebbero avuto piu' velocita' di navigazione sulla rete... 8-0
Molte persone hanno cambiato operatore, molte erano giunte al punto di arrivare ad una causa legale solo perche' a loro, la connessione internet serviva davvero, ma le reti mobili e le key erano di tutt'altro parere...

Concludo dicendo che le reti mobili saranno il futuro di internet, per cui, dove in un'epoca come la nostra, in cui le persone tolgono la linea telefonica di casa e passano ai cellulari, mi sento di dare un consiglio a tutti gli operatori di rete mobile italiani: avete in mano il futuro della rete, fate i bravi e dateci tutta la tecnologia che ci serve per navigare bene e sempre meglio. :-))

Di nuovo a tutti voi, buona navigazione ;-))

Computer Forensic: il sistema DEFT Linux

Post n°12 pubblicato il **13 Maggio 2012** da exodus1984
Carissimi bloggers, oggi parleremo di come viene usato un sistema GNU/Linux in ambito forense, in particolare della distribuzione DEFT Linux 7 "Arcana Intellego" - Release i386.

Per capire l'uso di una distribuzione di questo tipo, dobbiamo prima vedere il campo applicativo del suddetto sistema, questo tipo di sistema operativo, viene usato per il computer forensic, ovvero per trovare le prove di crimini informatici e non solo per questo, i crimini possono essere anche di natura diversa, ma con collegamenti di rete che potrebbero indicare il colpevole in modo certo.

Fare una analisi di un crimine informatico richiede una buona preparazione e l'uso di strumenti dedicati, questi, possono portare le prove certe di un solo presunto atto di vandalismo informatico, ma questo non e' tutto, trovare le prove effettive e certe di un crimine informatico o legato all'ambiente IT, richiede una ricerca minuziosa dei particolari che sono diversi da un caso ad un altro, e quindi, ci si deve muovere sempre con moltissima attenzione.

L'uso che ne' potete fare della DEFT Linux, vi consentira' di capire e trovare (quasi) tutte le prove che cercate per confermare o meno la colpevolezza di un vostro cliente implicato in qualche caso di questo tipo.
Dicevo, quasi tutte le prove, perche' se l'utente indagato puo' avere delle conoscenze informatiche avanzate, sara' molto difficile trovare qualche informazione utile che possa provare il crimine a lui attribuito.

Potete trovare informazioni in rete al riguardo di DEFT Linux, potete leggere molti manuali e potete scaricarvene una copia per provarla in modo concreto e utile per apprendere il suo funzionamento.
Di distribuzioni di questo tipo, dedicate appunto al computer forensic, potete trovarne molte, e ognuna con le sue caratteristiche particolari.

Ritornando al nocciolo della questione, l'uso di una distro linux come DEFT, vi permette di recuperare molti dati utili per le vostre indagini, ma allo stesso tempo, e' una lama a doppio taglio.

Mettiamoci nei panni di un criminale informatico:

punto 1)
conoscendo le tecniche usate nel computer forensic, si puo' aggirarle e preparare le prove che poi verranno "scoperte" sui PC degli indagati.

punto 2)
il criminale informatico di solito prevede con largo anticipo le mosse
degli investigatori, questo per garantirsi una via di fuga veloce e sicura.

punto 3)
il criminale informatico e' sempre anonimo, e conosce perfettamente le tecniche adatte per mantenersi anonimo, facendo ricadere tutte le tracce su sistemi diversi e gia' compromessi in precedenza per questo uso.

Si potrebbe scrivere un'intera biblioteca sulle tecniche usate e sui sistemi di violazione, fino alle contromisure usate dalle varie polizie del pianeta, e questo, i criminali lo sanno molto bene.
Per cui, se desiderate imparare qualcosa di utile, vi consiglio di provare la DEFT Linux, ma non solo, cercate in rete anche altre distribuzioni Linux di questo tipo, e soprattutto, usatele per apprendere.

Ricordate che la conoscenza e' potere, e questo potere deve essere usato bene, perche' la rete e' nostra e abbiamo il diritto di difenderci da tutti gli attacchi che potremo subire, quindi, imparate ad usare questi sistemi e gli strumenti che ci vengono messi a disposizione per farlo.

Si vis pacem, para bellum...

in hoc signo vinces ;-)))

E con questo cari bloggers, concludiamo questa prima parte dedicata alle distribuzioni GNU/Linux e al loro uso specifico nella vita di tutti i giorni, a tutti voi, di nuovo buona navigazione :-)

Distribuzioni Linux: il sistema SolusOS per PC vecchi e nuovi

Post n°13 pubblicato il **15 Maggio 2012** da exodus1984
Carissimi bloggers, oggi proseguiremo con le recensioni d'uso dei sistemi operativi Linux piu' usati del momento.

Iniziamo con SolusOS, un sistema basato su Debian che permette l'uso di key USB e supporti live, includendo supporti DVD,video e musicali con un'installazione adatta ai computer "antichi", ma creata espressamente per i nuovi modelli di PC.

Eccovi il link dove potrete scaricarla:

http://solusos.com/download/

Come tutte quante le altre distribuzioni Linux, anche questa dispone di supporto forum, irc, blog e community mondiali di discussione e sviluppo.
La stabilita' del sistema e' stata messa al primo posto, poi abbiamo i supporti per i gamers 3D e molto altro ancora.
Vi invito a scaricarla e a provarla personalmente, cosi' potete capire come potrebbe esservi utile in qualche modo.

Sul sito, alla sezione blog, potete vedere le news del sistema oppure i nuovi pacchetti pronti in repository.
Per emularla su un computer di test, potete usare il classico terminale Linux digitando il seguente comando, che a seconda della piattaforma che avete, vi fornira' subito un'anteprima del sistema operativo in esecuzione simultanea al vostro Linux preferito:

qemu -cdrom SolusOS-1.iso

Per elencare solo alcuni tipi di programmi, abbiamo il Minitube, un lettore veloce per video youtube, con diverse possibilità di applicazione dei video, poi sul desktop principale abbiamo la classica cartella HomeLive, il sistema di installazione su disco, il centro di controllo per il monitor e i driver video accellerati, e molte altre opzioni che possono essere installate facilmente da programmi grafici di scelta dei singoli pacchetti.

Questo sistema operativo e' davvero superiore ad altre distribuzioni Linux piu' "grosse", ma sotto alcuni aspetti, e' carente di altre piccole cose che possiamo appunto ritrovare su distribuzioni Linux piu' conosciute e usate di questa, ma credo che se questo fenomeno persiste, questo sistema operativo fara' davvero molta strada, finche' non ne' potremo piu' fare a meno.... ;-)))

Cari bloggers, anche per oggi e' tutto, buon web a tutti voi e se potete farlo, usate sempre i prodotti OpenSource, perche' al giorno d'oggi sono la cosa migliore che potete avere senza farvi spennare da ben note aziende con licenze inutili e restrittive... ;-))

Firme elettroniche: immagini e contenuti sul Web, miniguida fai da tè ;-)

Post n°14 pubblicato il **16 Maggio 2012** da exodus1984
Carissimi bloggers, oggi parliamo di firme elettroniche, ovvero come firmare un file che ci appartiene del tipo immagini jpg, gif, bmp, documenti pdf, etc etc. .

Nella gran parte dei casi si possono utilizzare chiavi create da programmi appositi oppure create da noi stessi e quindi cifrate.
Il problema che si pone e' che una firma di questo tipo, potrebbe essere contraffatta e farci perdere cosi' la proprietà' del nostro file.

Sui moderni sistemi Linux, possiamo farlo in diversi modi, possiamo cliccare ad esempio sull'immagine che dovremo mettere sul nostro sito web, oppure che dovremo postare sul nostro blog ed infine cliccare su "Firma", questo comando ci permette di firmare elettronicamente un documento avendo gia' creato in precedenza una chiave con la quale potremo sapere se il nostro file e' a posto oppure no. :-)

Per molto tempo le immagini internet hanno trasportato messaggi nascosti al loro interno, pur funzionando bene comunque.
L'uso che ne' viene fatto ancora oggi, puo' suggerirci il modo per creare una firma del tutto personale per le nostre immagini, garantendo sempre la qualita' e la (quasi) proprieta' delle stesse.... ;-))

Possiamo creare una firma personale partendo da un semplice file di testo in cui scriveremo i nostri dati di proprieta' dell'immagine che vogliamo mettere su internet:

create il file di testo:

parsec@exodus84:~$ touch firma.txt
###############

editate il file di testo:

parsec@exodus84:~$ vi firma.txt
###############

al suo interno inserite i vostri dati:

fotografia n# 10000000
autore: Tapiro de Tapiris
Via del Tapiro Informatico n#84
ora: 00:00:00
numero di scarpe: 84
numero di telefono: 8484848484... ;-))
.....
...

Quando avete finito, per uscire premere ESC, quindi digitare :wq e premere invio.

Cifrate i vostri dati con l'ausilio di GPG:

parsec@exodus84:~$ gpg -c firma.txt

ora avremo a disposizione due files con il nome quasi uguale:
firma.txt e firma.txt.gpg.

Potete notare che non abbiamo creato chiavi condivise, ma abbiamo utilizzato un cifrario simmetrico, usando una password che sara' conosciuta solo da noi e non avremo chiavi condivise con nessuno.

A questo punto possiamo dare il seguente comando da terminale:

parsec@exodus84:~$ cat firma.txt.gpg >> tapirotruccato.jpg

Cio' che facciamo e' molto semplice, aggiungiamo il codice cifrato all'interno del file immagine, che avra' un relativo aumento di peso(pochi Kb), ma la struttura dell'immagine non verra' modificata, permettendo a tutti di vederla, ma senza che nessuno sappia quello che contiene, ad una successiva verifica, potete usare un semplice editor esadecimale per estrarre la vostra firma, rivendicando il vostro diritto

sull'immagine stessa. ;-))

Bisogna dire che pero' questo metodo e' un metodo piuttosto semplice, e che se guardate bene in rete, potrete trovare di meglio, ma per chi di voi vuole fare pratica con i comandi al terminale di Linux, questo e' senz'altro un buon modo di iniziare. ;-)

E anche per oggi e' tutto cari bloggers, e come sempre, auguro a tutti voi una buona navigazione su internet. :-)

Siti Web personali: creare una semplice pagina personale su Libero.it

Post n°15 pubblicato il **18 Maggio 2012** da exodus1984
Carissimi bloggers, oggi impareremo a creare una pagina web, navigando tra i blog di Libero, ho notato che molti attivano lo spazio Web ma non lo usano nel modo corretto per condividere le informazioni oppure semplicemente non sanno come dovrebbe essere usato.

Ho scritto questa piccola guida perche' molte persone vorrebbero avere anche una pagina Web oltre che il loro semplice profilo, ma non sanno usare gli strumenti che Libero mette a disposizione, oppure non hanno dimestichezza con la programmazione manuale di un sito Web.
In ogni buon caso, il mio consiglio e' che almeno una volta, una volta sola, proviate a leggere le guide che Libero mette a disposizione degli utenti dei suoi blog e siti web, imparerete molte cose utili.

Benche' ci siano milioni di guide per la creazione di siti Web, le persone non hanno voglia di perdere il proprio tempo in letture tecniche mentre se' ne' vanno in giro sulla rete a divertirsi, e quindi ho pensato bene che se leggete solo blog, allora vi offro questa piccola guida che spero vi sia utile perche' possiate divertirvi davvero a creare le vostre pagine web :-)

In questa breve guida, voglio illustrarvi alcuni semplici passaggi per creare la vostra prima pagina Web su Libero.it .
Cercheremo di essere molto concisi, in modo da far capire alle persone che leggono questo articolo come ottenere la pagina web che desiderano, ma anche per fare delle prove e dei test per tutti quelli che desiderano imparare a crearsi un piccolo sito Web fatto tutto "a mano", anche se Libero mette a disposizione applicazioni grafiche per la costruzione dei siti che sono davvero molto intuitive nel loro uso.

Oggi impareremo a creare una(1) sola pagina Web, basata esclusivamente sul file indice ovvero: index.html .
Useremo questo file come esempio di partenza, infatti, possiamo creare un enorme file index.html, oppure possiamo scegliere se dividere il nostro sito Web in pagine secondarie, come se sfogliassimo un libro, non voglio entrare affatto in terminologie tecniche che potrebbero spaventare gli utenti alle prime armi con il Web, per cui, le istruzioni che seguiranno, cercheranno di essere molto brevi perche' possano essere comprese subito da tutti gli utenti non "tecnici".

Come prima cosa, sul nostro pc casalingo, dovremo creare una directory dove terremo per il momento tutto il materiale che ci serve, in futuro, imparerete certamente a dividere le directory del vostro sito Web, le foto, i documenti che volete condividere con il resto del mondo.

Iniziamo la costruzione della nostra prima pagina Web.

Create una directory di partenza dove poter lavorare, per esempio:
myliberoweb, aprite un terminale e createla:

parsec@exodus84:~$ mkdir myliberoweb
####################################
quindi inseritevi nella nuova directory per iniziare il lavoro:

parsec@exodus84:~/myliberoweb$
##############################
ora, create il file "index.html" richiesto dal motore Web di Libero:

parsec@exodus84:~/myliberoweb$ touch index.html
##
adesso, editate il file indice:

parsec@exodus84:~/myliberoweb$ vi index.html
##

ora, scriveteci dentro il codice:

<body style="color: rgb(0, 0, 0); background-color: rgb(255, 255, 255);" alink="#000088" link="#0000ff" vlink="#ff0000">

```
<br><br><br>
<div align="center">
<em>
Questa e' la nostra prima pagina Web, fatta a mano e made in italy... ;-)))
</em>
</div>
```

quindi premete ESC, digitate :wq e premete INVIO, a questo punto, la nostra prima pagina Web e' stata creata, adesso dobbiamo mandarla sul server di Libero.it perche' possa essere condivisa:

```
##################################################
parsec@exodus84:~/myliberoweb$ ftp ftp.digiland.it 21

Connected to digi-ftp2.iol.it.
220 195.210.93.35 FTP server ready
Name (ftp.digiland.it:parsec): exodus1984
331 Password required for exodus1984
Password:
230-Benvenuto sul server FTP delle pagine personali di Digiland!
 Bytes disponibili per upload 152076288.
230 User exodus1984 logged in
Remote system type is UNIX.
Using binary mode to transfer files.

ftp> put index.html  <--usate questo comando FTP :-))

local: index.html remote: index.html
200 PORT command successful
150 Opening BINARY mode data connection for index.html
226 Transfer complete
459 bytes sent in 0.00 secs (12114.7 kB/s)
ftp> exit
221 Goodbye.
#
parsec@exodus84:~/myliberoweb$
##################################################
```

Noterete che abbiamo usato il comando "put" per inviare alla cartella con il nostro nickname il file index.html, adesso se cliccate sulla barra in alto del vostro profilo, sulla dicitura "SITO" potrete vedere il risultato del lavoro che avete appena fatto, avete creato la vostra prima pagina Web!!

Per vedere questa pagina in "azione", cliccate sulla dicitura "SITO", quando visitate il mio blog o profilo :-)

Cari bloggers, spero che questa piccola e veloce guida, possa servire come punto di partenza per le persone che non conoscono la programmazione di base delle pagine Web, a tutte queste persone voglio dire che c'e' sempre tempo per imparare, basta solo applicarsi se lo si desidera veramente. :-))

In fondo, il Web non e' altro che testo, puro testo formattato in modo tale da risultare con una definizione migliore del testo stesso... ;-)

Carissimi bloggers, anche per oggi e' tutto, auguro a tutti voi un buon fine settimana e ci ri-leggiamo ai prossimi articoli ;-)))

Ricordi non ancora svaniti: i terremoti in Italia

Post n°17 pubblicato il **20 Maggio 2012** da exodus1984
Un veloce post per portare la mia solidarieta' a tutte le persone colpite dal terremoto in Emilia e dintorni, nel 1976 ho vissuto in prima persona il disastroso terremoto del Friuli(6 maggio 1976), e so' molto bene come ci si sente dopo un'esperienza di questo tipo, ho ancora moltissimi ricordi, alcuni stampati in modo indelebile anche nell'orto che coltivo vicino a casa, in cui una devastante frana ha portato massi grandi come case a depositarsi proprio qui, in perenne ricordo di quell'evento.

A tutte le persone colpite da questo terremoto, la mia piena solidarieta' e un augurio di buona fortuna perche' possano riprendersi al piu' presto da quanto è successo.

Italia di oggi: analisi e psicologia di un attentato

Post n°16 pubblicato il **20 Maggio 2012** da exodus1984
Carissimi bloggers, oggi 19 maggio 2012, e' una giornata triste per l'Italia, una giovane ragazza che non tornera' piu' a casa, altri feriti gravi e tutti quanti, vittime innocenti di una mano omicida senza scrupoli... :-(

Tutto questo mi spinge a scrivere un veloce articolo e a postarlo sul blog in tutta fretta per esprimere la mia totale disapprovazione per tutto questo.

Si sta' indagando sulla costruzione di una bomba del genere per trovare il colpevole, ma le cose saranno alquanto difficili, se non impossibili...
Purtroppo, conoscendo il comportamento di questi soggetti, posso dire che non solo sara' del tempo perso, ma permettera' ai veri colpevoli di rimanere impuniti... almeno questa volta, speriamo che possano essere davvero presi...

Mafia? Organizzazioni Eversive?? Servizi Segreti deviati??
Molte volte mi sono chiesto il perche' di tutto questo, e forse la risposta giusta e' quella piu' semplice...:-(

Nello studio psicologico del caso in questione, si puo' evincere un chiaro segno di pianificazione dell'attentato che porterebbe a pensare ad un'organizzazione terroristica, ma molti di questi comportamenti, possono essere indotti, ovvero: creare e pianificare un attentato di questo tipo, richiede un minimo di preparazione e di conoscenza di base dei vari componenti esplosivi che si vogliono usare, non di meno la conoscenza degli inneschi che possono essere usati.
Inoltre, creando un ordigno di questo tipo, e sapendo come condurre una guerra psicologica, si puo' portare gli inquirenti a pensare cio' che gli attentatori vogliono che pensino, mi spiego meglio:

costruendo un ordigno "rudimentale", gli inquirenti verranno "deviati" da un'organizzazione terroristica che secondo il loro pensiero, non potrebbe costruire ordigni di cosi' "basso livello qualitativo".

costruendo un ordigno "professionale", ovvero con dispositivi d'innesco a micro-elettronica e sistemi anti-artificiere, gli attentatori possono portare l'attenzione degli inquirenti verso gruppi e celle terroristiche di matrice estremista, deviando l'attenzione dei veri responsabili di questa strage che potrebbero non avere nulla a che vedere con il terrorismo.

Tutto questo, mi fa' davvero pensare a strane coincidenze che mi ricordano fatti gia' accaduti e di cui sono stato testimone diretto in moltissime occasioni.
Ho fatto queste considerazioni, in base alla mia esperienza dopo molti anni di studio su diversi casi di questo tipo, le mie idee, possono essere non apprezzate da tutti, ma questo e' il mio pensiero di oggi, e ho voluto condividerlo con tutti voi.

Riflessioni personali psicosocial_attapirate: un mondo tutto mio.... ;-)))

Post n°18 pubblicato il **21 Maggio 2012** da exodus1984
Carissimi bloggers, oggi solo un veloce saluto a tutti voi mentre sto' pensando a scrivere nuovi articoli che possano essere utili a tutti.

Oggi devo pensare a come impostare il sito web, in modo da farvi vedere qualche bella foto "webbizzata".

Sto' preparando alcuni articoli da pubblicare e sono pertanto preso dallo studio dei contenuti, speriamo che ce' la faccio...;-)

Buona navigazione a tutti voi . :-)

Italia di oggi : la psicologia comune del "Capro espiatorio"

Post n°19 pubblicato il **22 Maggio 2012** da exodus1984

Carissimi bloggers, questa sera volevo mandarvi un articolo sulla creazione di un sito web personale, ma' la mia etica mi impone di scrivere qualcos'altro.

Nei giorni scorsi, dopo la bomba di Brindisi, si sono dette molte cose al riguardo del presunto colpevole, oggi, scrivo questo semplice articolo per portare la mia solidarieta' al presunto "colpevole", ancora una volta, la giustizia italiana e' riuscita a rovinare la reputazione di una persona normale e a perdere di nuovo la strada.

Con questo articolo, non voglio denigrare il lavoro svolto dagli inquirenti, ma vorrei far capire a tutti, giustizia, stampa e politica italiana, che questa non e' la strada giusta da seguire: un capro espiatorio in un caso di questo tipo serve sempre per coprire le tracce dei veri colpevoli, ma questo, poco importa, perche' la giustizia deve far vedere ai cittadini italiani che funziona, la stampa italiana non e' da meno, tutti come avvoltoi su una notizia per essere i primi a pubblicarla... :-(
Che poi, il "sospettato" sia colpevole o meno, non ha la minima importanza, l'importante, e' dare la notizia, ma vediamo come:

durante un'indagine di questa portata, tutte le informazioni, devono essere segrete, quindi le fughe di notizie devono essere condannate e represse con decisione, ma purtroppo esistono persone anche all'interno dei vari reparti investigativi, che "parlano troppo", e cosi' si creano le notizie che arrivano sugli schermi degli italiani.

Ci sono poi anche quelle persone che per soldi, tengono i piedi in due scarpe diverse, ovvero: lavorando per un caso di questo tipo, "arrotondano" fornendo particolari d'indagine ad alcuni giornalisti senza scrupoli, che creano un articolo "esclusivo", e sono subito seguiti a ruota da tutte le altre testate giornalistiche nazionali che come sempre, ingigantiscono la notizia originale e creano guai seri ai "sospettati" e alle stesse indagini del caso.

Ricordo a tutti voi che il "sospetto", non genera affatto certezza di reato finche' non ci sono prove valide e schiaccianti, se' ce' una cosa che ho potuto imparare bene, e' che prima di dire "e' lui, prendetelo!!!", bisogna essere davvero sicuri di quello che si sta' dicendo, perche' altrimenti succede che la giustizia italiana ci fa sempre una brutta figura.

Per cui, invito tutti quanti voi a pensarci sopra, e parlo perche' conosco bene queste situazioni.
Un vecchio detto racconta che la fretta e' una cattiva consigliera, e che la pazienza e' la virtu' dei forti...
Allora, meditate gente, meditate sui casi della vita, perche' se continuate cosi', non arriverete a nessuna conclusione.
Lo avevo gia' affermato in un mio articolo precedente, ma ormai, so' bene come vanno queste cose... :-(

Un PS per gli inquirenti che sono su questo caso:

piu' della meta' degli italiani ha un diploma in informatica ed e' esperto di tecnologie elettroniche, allora siamo tutti sospettati???
Personalmente, ho un ottimo addestramento CBRN, allora, sono un terrorista anch'io??? Ma fatemi il piacere...
Nei primi tempi di questo caso, si e' parlato di immagini ad altissima risoluzione grafica, ma poi, sentendo che serviva un identikit del presunto "colpevole", ho visto subito che qualcosa non tornava in tutte queste informazioni.

Un PS per la stampa nazionale:

fate attenzione alle notizie che date, come si diceva una volta, prima della tastiera del computer: la penna uccide piu' persone di una spada affilata...

Con questo, cari bloggers, vi lascio a meditare sui casi della vita, e auguro agli inquirenti che indagano sulla bomba di Brindisi, di ritrovare al piu' presto la strada perduta e alla stampa nazionale di ritrovare la propria etica professionale, che ultimamente vedo che e' un pochino persa...:-(

A tutti quanti voi, come sempre, buona navigazione.

Eventi pianificati: la psicologia e il controllo informativo

Post n°20 pubblicato il **26 Maggio 2012** da exodus1984
Carissimi bloggers, eccoci di nuovo qui a bloggare articoli di varia natura e contenuti diversi ogni volta. :-)

Dal ritorno dopo tanto tempo passato altrove, su reti e sistemi diversi, oggi
vi voglio raccontare la storia (infinita) della psicologia applicata al pensiero umano, che genera comportamenti indotti negli individui comuni portandoli a fare cose che altrimenti non potrebbero essere mai fatte dalle persone.

Quello che voglio raccontarvi oggi, e' uno degli episodi in cui mi sono trovato immerso fino al collo, un caso che era praticamente risolto in partenza, ma che per mancanza di prove fisiche, aveva richiesto diversi mesi di indagini su un ampio campione di persone.

I soggetti interessati in questo caso, avevano un'eta' tra i 18 e i 22 anni, e la complessita' delle relazioni interpersonali tra il campione posto sotto test e quello definito con conoscenze informative dirette, erano molto vicine ad un'affinita' collettiva parificata.

Usare la psicologia applicata ad ognuna delle persone poste sotto test per generare un evento fisico predefinito e valutare cosi' la possibilita' di poter indurre un particolare evento, predisposto in precedenza per il suddetto test.
Cosi' facendo, si potevano ottenere informazioni diverse dai vari gruppi di test, cambiando semplicemente l'obiettivo finale, ovvero: se si voleva ottenere determinate informazioni, si testava il comportamento comune del soggetto sotto test per capire dove poter intervenire, inducendo il comportamento che il soggetto doveva avere per arrivare alla fine del test da solo puntando all'obiettivo predefinito.

Non posso sapere se questo semplice articolo puo' interessare o meno la comunita' dei bloggers, ma oggi ho voluto condividere con tutti voi qualcosa che mi ha portato ad essere quello che sono, e che ancora una volta, mi ha aiutato nei difficili casi che la vita ci propina continuamente, mettendoci continuamente alla prova giorno per giorno.

Ho scritto questo articolo per accontentare alcuni vecchi amici che da tempo mi assillano con richieste di questo tipo, ma che per il mio pochissimo tempo a disposizione, non sono mai riuscito a mandare su questo blog.

Cari bloggers, un saluto a tutti voi e come sempre, buona navigazione e buon divertimento sulla grande rete :-)

La psicologia della persuasione collettiva: esiste davvero la liberta' di pensiero?

Post n°21 pubblicato il **27 Maggio 2012** da exodus1984
Carissimi bloggers, anche oggi vi mando qualcosa da leggere su cui potrete meditare fino alla prossima volta.

Oggi parliamo di messaggi subliminali, ovvero messaggi indotti ad ottenere crediti presso qualsiasi azione venga svolta.
Iniziamo con una banale notizia presa da internet, il terrorismo di nuova generazione.

Questo nuovo stile, definito cosi' dai maggiori personaggi che operano per la sicurezza nazionale italiana, sembrerebbe utilizzare diverse tecniche usate in passato da altri gruppi eversivi, e' anche vero che esistono reti e sistemi "nascosti" sui quali i nuovi manager del terrore italiano operano da diverso tempo, ma chissa' perche'pur disponendo di questo tipo di informazioni, nessuno ci puo' fare nulla... :-(

Allora analizziamo bene la cosa, se i servizi segreti italiani mettono sul Web informazioni di questo tipo che dovrebbero essere tenute segrete per i ben evidenti problemi di sicurezza, allora esiste un ben valido motivo perche' si possa arrivare a questo: specificando prima gli obiettivi che dovranno essere colpiti, si puo' inviare un messaggio subliminale ai cittadini italiani del tipo:" ti dico adesso dove esplode la bomba, cosi' dopo capirai che ho detto la verita'..."
Alcune delle informazioni che comunque sono state date per la gioia dei navigatori del Web, provengono da archivi molto vecchi, risalenti a non piu' di 15-20 anni fa'. Tutto questo ci porta a pensare ad azioni che potrebbero compromettere seriamente la liberta' dei cittadini italiani. Sappiamo che e' gia' successo in passato, ma nulla si puo' escludere per il nostro futuro.

Premetto che io rispetto tutti, ma conoscendo bene alcune situazioni molto particolari, non giudicatemi male se non mi fido quando sento informazioni che dovrebbero essere tenute segrete, e che invece, vengono distribuite con dosi anche molto eccessive di particolari tecnici sul "dove, come e quando".

La mia etica professionale mi impone di scrivere un chiarimento come questo, non perche' possa essere letto qui sul blog, ma per far capire ad alcune mie vecchie conoscenze che siete completamente fuori strada, e i casi sono solo due: o lo fate apposta, oppure siete davvero arrivati alla frutta mettendo sul Web notizie come queste... :-(
Dove e' finita l'etica professionale? E il segreto istituzionale?

Per cui, il terrorismo di nuova generazione potrebbe incamerare le scuole di pensiero di gruppi rivoluzionari vecchi e nuovi, ma questo e' gia' successo molto, molto tempo fa'... :-(
Il "reclutamento" di nuove leve??? Roba vecchia, ce' sempre stato un ricambio generazionale in ogni organizzazione di questo tipo...:-(

E potrei continuare ancora, ma per oggi basta cosi', vorrei ritornare a scrivere qualche bell'articolo sui computer, senza pensare troppo a questo genere di notizie, pero' vedere l'italia violentata in questo modo e i suoi cittadini presi per degli stupidi idioti, mi fa' arrabbiare molto.
Il "nuovo terrorismo" potrebbe essere davvero anche fatto cosi'?

E mentre il capo della polizia afferma che: "gli anarchici sono il vero pericolo per il paese", qualcuno sta' tramando nell'ombra, ma non credo che di anarchici si possa trattare... :-(
Mi chiedo di questo passo che fine fara' la mia bella Italia, maltrattata da tutte le parti in causa... :-(

Come sempre cari bloggers, buona navigazione a tutti voi

Cucina veloce: cosa mangiamo oggi?

Post n°22 pubblicato il **28 Maggio 2012** da exodus1984
Carissimi bloggers, oggi parliamo di cucina, per la precisione, oggi cucineremo le pennette al burro,grana e gorgonzola, in seguito, prepareremo il dolce con le fragole di stagione e il vino bianco.

Allora andiamo a preparare tutto quello che ci serve, gli ingredienti sono per quattro(4) persone:

Fate cuocere 250 grammi di mezze penne di pasta di semola di grano duro, la cottura ottimale e' circa di 9/10 minuti, se desiderate avere la pasta piu' molle e non al dente, potete semplicemente spegnere i fornelli e lasciare che la cottura prosegua ancora un po' prima di scolare la pasta.
Se invece volete avere una pasta al dente piu' "dura", fermate la cottura con due bicchieri di acqua fredda e quindi preparate il tutto per il condimento finale.

Dovrete avere gia' preparato il condimento, preparate in tre piatti diversi del burro, delle scaglie di Grana grattuggiate a coltello in modo che siano poi visibili sul piatto finito.
Quindi tagliate una fetta di Gorgonzola dello spessore di 3/4 centimetri e ora proseguite alla preparazione del piatto finale.

Fate sciogliere il burro in un piccolo contenitore di metallo, ricordate che dovrete solo sciogliere il burro e non farlo friggere, mantenendolo pero' ad una temperatura ne' troppo fredda, ne' troppo calda.

A questo punto, prendete la pentola che contiene la pasta gia' scolata, rimuovete il coperchio e quindi versateci il burro caldo girando le mezze penne con una spatola di legno mentre versate.

Ora che il burro caldo ha impregnato le mezze penne, inseriteci la vostra fetta di Gorgonzola che avevate preparato in precedenza, sempre continuando a girare il tutto con la spatola di legno in modo che il Gorgonzola si possa in parte sciogliere.

Adesso, servite il piatto caldo e varsateci sopra ad ogni porzione le scaglie di Grana in modo che i sapori finali possano essere sentiti e associati dai vostri ospiti.

##

Prepariamo il dolce finale, per questa preparazione, sono richiesti quattro(4) ingredienti, necessari per la buona riuscita.

un cestino di fragole mature
vino bianco dolce
limone
zucchero

Pulite le fragole dal picciolo, mettendole per una ventina di minuti nell'acqua dove avrete sciolto due cucchiaini di bicarbonato per usi alimentari.
Togliete l'acqua di pulitura e risciaquate tutte le fragole con acqua corrente fredda e quindi cominciate a tagliarle in quattro(4) pezzi longitudinali.

Preparate il succo finale aggiungendo due bicchieri di vino bianco dolce,
aggiungete il succo di limone spremuto in precedenza a seconda dei propri gusti, ed infine correggete il tutto sciogliendo alcuni cucchiaini di zucchero per rendere il succo finale dolce ma con punte acide che esaltano il sapore delle fragole.

Lasciate raffreddare in frigorifero per alcune ore, poi servite con una spruzzata di panna spray oppure assieme al gelato che avrete preparato.

Cari bloggers, buon appetito a tutti voi e buona navigazione

Sistemi Operativi: AntiX Linux, recuperiamo i vecchi computer con stile e professionalita'

Post n°24 pubblicato il **29 Maggio 2012** da exodus1984
Carissimi bloggers, oggi useremo un nuovo(si fa' per dire...) sistema operativo basato come sempre sul kernel Linux.

Questa piccola distribuzione, si chiama ANTIX, e potete trovarla a questo indirizzo web:

http://antix.mepis.org/index.php?title=Main_Page

Appena siete giunti su questa pagina, cliccate su "Download", per avere una panoramica di scaricamento completa dei vari .iso della distribuzione.
Questa distro, vi permette di non buttare via i vostri vecchi computer, percio' anche se' avete un pc con qualche anno sulle spalle e non potete piu' aggiornare il vostro sistema windows perche' non piu' compatibile con questa macchina, dovrete solo buttare il sistema windows e reinstallare questa distribuzione, che incorpora tutte le piu' moderne tecnologie, ma che allo stesso tempo, si possono usare benissimo su tutti i computer datati.

Potete controllare le firme MD5 e le varie distribuzioni su sourceforge.net a questo indirizzo:

http://sourceforge.net/projects/antix-linux/files/Testing/

le firme MD5:

Files uploaded 26 May 2012.

527527d1193f7ff64e194aecaabb4e87 antiX-base-486.iso
a28c5e3ac7099c0e100af2156dc210f4 antiX-core-libre-486.iso
53e3a57e2ef19e27abeae109116c0f3e antiX-486.iso

Per il resto, seguite i mirror che vi vengono proposti per scaricare il file .iso da masterizzare poi su un normale Cdrom.

Se volete guardare il video di presentazione del sistema operativo, potete andare a questo link:

http://www.youtube.com/watch?v=8jIHGT4gYXc

A tutti voi, buona navigazione e buon divertimento ;-))

il Presidente Napolitano in Friuli

Post n°23 pubblicato il **29 Maggio 2012** da exodus1984
Cari bloggers, oggi ci sara' la visita del presidente Napolitano qui a Gemona, in ricordo del terremoto del 1976 e ulteriori visite in ricordo dei caduti della resistenza partigiana nella seconda guerra mondiale.

Per cui, un veloce post per ricordare a tutti voi che l'italia e' un grande paese, e la mia regione, il Friuli, lo ha ampiamente dimostrato durante tutti questi eventi storici.

Di nuovo, un saluto a tutti voi e buona navigazione su internet :-)

Sistemi Operativi: migliorare Windows con il software Open source

Post n°25 pubblicato il **30 Maggio 2012** da exodus1984
Carissimi bloggers, oggi prenderemo in considerazione l'uso di software Open Source che potete usare su Linux portato pero' su sistemi operativi windows.

Il motivo di questa scelta e' quello di far conoscere a piu' persone possibili il mondo OpenSource, e visto che la grande maggioranza di navigatori usa il sistema operativo Windows, oggi cercheremo di renderlo migliore, sfruttando alcuni software liberi che normalmente, potremmo trovare solo su sistemi Gnu/Linux, ma non solo su questi.

Per potervi scaricare un supporto cd/dvd, dovrete linkare i seguenti indirizzi web, se volete provare un solo cdrom con alcune applicazioni per vedere se vi puo' servire (650 Mb di download):

http://linux.studenti.polito.it/download.php?version=297

il codice version=297 identifica il supporto cdrom.

################################

Se avete provato il cd e siete rimasti soddisfatti, allora puntate direttamente al dvd completo (1,6 Gb di download):

http://linux.studenti.polito.it/download.php?version=298

il codice version=298 identifica il supporto dvd completo.

################################

Il dvd contiene varie utility per windows, programmi che possono essere davvero utili se non potete spendere una cifra per procurarvi un software commerciale equivalente.

Tutti i programmi sono selezionati per utilita' specifica, ovvero: navigatori web, applicativi office, player video e audio, utility di sistema, e molto altro ancora.

Se invece volete una selezione di software portatile, ovvero senza installare nulla sui vostri sistemi windows, allora dovete usare la distribuzione TheOpenDrive, scaricabile a questo link (575-557 Mb di download):

http://linux.studenti.polito.it/downloadtodrive.php

################################

Vorrei invitare tutti quanti voi a scoprire e provare questi programmi che sicuramente daranno una marcia in piu' al vostro sparuto sistema windows :-)

Molte di queste utility, mi hanno aiutato a risolvere dei problemi sui sistemi windows, ma ho potuto anche lavorare con programmi per la creazione di calendari personalizzati e modificare delle fotografie senza usare prodotti costosissimi che normalmente, vengono venduti per questo sistema operativo.

Il valore di tutte queste applicazioni e' molto alto in termini di qualita' e di risparmio per gli utenti windows, e quindi per ottenere lo stesso risultato con programmi commerciali, dovreste spendere un capitale per avere le stesse applicazioni che qui vengono fornite con codice aperto a tutti.

Molti di voi, potranno ribattere che i programmi commerciali sono migliori, pero' io vi posso dire che se siete "solo" utenti normali sui sistemi windows, allora questa suite e' piu' che sufficiente per voi, ma vi posso garantire che molti professionisti che conosco usano regolarmente queste applicazioni sui loro sistemi windows, e quindi, e' solo questione di effettuare una scelta, una scelta che penso possa cambiare la vostra vita lavorativa sui sistemi informatici windows.

Ho scritto questo semplice articolo per rispondere alle richieste di alcuni amici che mi chiedevano programmi di questo tipo, solamente per sistemi Windows, se in ogni caso girate la rete, potrete trovarne molti altri che possono esservi utili, questo e' solo un piccolo assaggio di quello che potete avere risparmiando tempo e denaro, e ottenendo sicuramente qualcosa in piu' dai vostri sistemi Windows.

E per chi vuole farsi davvero una cultura, oppure a chi di voi piace leggere o ascoltare musica classica, consiglio di visitare il seguente link, il portale della cultura italiana, in formato libero per tutti voi:

http://linux.studenti.polito.it/liberliber/

################################

E con questo cari bloggers, vi auguro una buona navigazione e buone ricerche su internet.

Riflessioni personali: il perche' di una scelta, dedicato agli amici e alle amiche reali e virtuali.

Post n°27 pubblicato il **03 Giugno 2012** da exodus1984
Carissimi bloggers, oggi vorrei dare qualche breve spiegazione al riguardo della mia presenza su questo blog.
Molti amici di rete(non bloggers), mi hanno chiesto in e-mail perche' ho fatto questa scelta, visto che conoscendomi bene, sanno che sono piu' il "tipo" da sito web che da blog. :-))

Oggi ho scritto questo articolo proprio per spiegare la mia "strana" presenza su un social network... ;-))
Questo articolo e' quindi piu' indicato per gli amici/amiche che mi conoscono da sempre che per i bloggers che navigano qui, ma ho scelto di postare qui i miei motivi non solo per spiegare agli amici che cosa ci faccio qui, ma anche perche' leggendo queste righe, anche i bloggers possano farsi un'idea di quello che voglio, di come sono, e soprattutto, di cosa sono venuto a fare qui.

Molti di voi, avranno visto che il mio blog non e' come gli altri, ovvero: senza fotografie, video, animazioni, questo perche' la mia essenza spirituale informatica, risponde ad un mio preciso desiderio di mantenere semplice e (quasi comprensibile...) tutto il materiale che invio qui.

Inoltre, non "collezionando" amici come fanno tutti sui vari social network, qualcuno si e' chiesto il perche' della mia presenza sul blog di Libero.
Per cui, adesso posso dare una valida spiegazione a tutti quanti, e per tutti coloro che nella mia presenza qui, notano qualcosa di "strano"... e questo, e' dedicato essenzialmente ai "vecchi volponi" che mi conoscono da sempre sulla grande rete ;-))

Allora, ecco qui:

Sono tornato dopo molti anni su Libero perche' i server di Libero sono appunto la mia seconda casa, e su questi server, e' stata scritta una buona parte della mia storia informatica personale, per cui, la mia, non e' stata la banale scelta di un provider a caso, bensi' di un effettivo "ritorno a casa" dopo moltissimi anni di assenza.

Lo scopo principale di questo semplice blog, e' quello di condividere con tutti la conoscenza che mi porto dentro, come faccio sempre nella vita reale di tutti i giorni, aiutando tutte le persone che hanno problemi con l'informatica e i computer in generale.
Mi piace scrivere, infatti ho scritto migliaia di guide sull'uso e l'abuso di internet, mi piace leggere, e i blog di Libero, sono davvero stupendi per questo. :-)

Essendo tornato qui con uno scopo ben preciso, ovvero: dare alla comunita' internet il mio contributo personale senza avere nulla in cambio per questo, cerco di esprimere quello che sono, cerco di migliorare la mia essenza informatica, la mia etica professionale mi impone di chiarire sempre i motivi di quello che faccio, e questa e' una forma di rispetto verso tutta la comunita' internet e le persone presenti che leggono i blog di Libero.

Il rispetto e' fondamentale per qualsiasi relazione interpersonale, sia che venga svolta qui su internet, sia che venga svolta nella nostra vita reale.
Questo ha portato alla creazione di questo blog "particolare", che altrimenti, non avrebbe potuto esistere.

Per cui, approfitto di questo articolo per ringraziare tutti gli amici e le amiche che conosco nella mia vita reale, e soprattutto in ricordo degli amici scomparsi con cui ho lavorato sulla grande rete per moltissimi anni, che mi hanno trasmesso tutte le loro conoscenze informatiche rendendomi una persona migliore e portando la mia banale esistenza ad un livello piu' alto nella scala evolutiva umana, facendomi comprendere il vero significato dell'universo.

Spero che con questo articolo tutti possano ritenersi soddisfatti, e allora cari bloggers e cari amici, a tutti voi, il solito e grande saluto augurandovi buona navigazione e buon divertimento su internet. :-))

Sistemi operativi: la leggendaria distribuzione Knoppix

Post n°26 pubblicato il **03 Giugno 2012** da exodus1984
Carissimi bloggers, oggi un veloce post ci porta a scoprire l'ultima grande release di una distribuzione Gnu/Linux che ha letteralmente cambiato il modo in cui un sistema operativo puo' funzionare.

Vi mando subito il link presso il quale potete scaricare questa live-distro e valutare cosi' se vi puo' interessare questo stupendo sistema Linux:

http://knopper.net/knoppix-mirrors/index-en.html

Sui mirror cercate questa immagine iso, scaricatela, masterizzatela e provatela :

KNOPPIX_V7.0.1DVD-2012-05-24-EN.iso

Questo post infatti, e' stato mandato utilizzando la nuovissima versione di Knoppix, ovvero la versione 7.0.1 per processori a 32 e 64 bit, una distribuzione Live che puo' essere usata senza installazione da dvd o da key usb.

Questo sistema dispone di moltissimi programmi per gli utenti live-on-line, per cui, e' molto consigliata per smanettoni/spippolamento/taroccamento internet/modifiche strane etc,etc... . ;-))

Il sistema viene settato al boot con i seguenti parametri del kernel:

knoppix lang=it desktop=gnome

oppure

knoppix64 lang=it desktop=kde

Il settaggio principale serve per avere un ambiente grafico sul quale si puo' lavorare o si lavora su qualche altro computer personale, e per il quale, si ha una dimestichezza particolare per il suo specifico uso, per cui la scelta dell'ambiente di lavoro e' tutta a livello personale o di esperienza, invece il settaggio della configurazione lang=it serve per poter utilizzare in modo specifico la tastiera e la localizzazione del kernel in lingua italiana.

La prima parte dei parametri del kernel di lancio del sistema, ovvero la dicitura knoppix/knoppix64, identifica l'architettura del processore, 32 o 64 bit, e le due modalita' sono diverse sotto molti aspetti, per cui prima di usare questa live-distro, dovreste almeno sapere il processore/i processori presenti sulla vostra macchina con le relative estensioni.

Questa versione dispone di parecchi aggiornamenti e debug, i programmi che sono presenti su questo dvd, servono per poter fare tutto quello che avete bisogno su qualsiasi computer voi stiate operando, senza toccare minimamente il sistema installato su quella macchina di default.

Questo sistema, permette di by-passare i sistemi windows, montare i relativi dischi fissi, e quindi di recuperare file e informazioni dai sistemi Ms che hanno problemi di avvio corrotto, e che devono essere re-installati completamente.

Su Knoppix, abbiamo moltissimi programmi utili, una potente suite di programmi per ufficio, un potente libre-CAD che ci permette di creare progetti e molte altre cose utili, poi per non dimenticare, disponiamo di una completa raccolta di software free per la modifica dei video e dei file audio in modo professionale, inoltre, una potente raccolta di software per lo sviluppo di applicazioni rende questo sistema una distribuzione portatile Linux davvero unica nel suo genere, benche' al giorno d'oggi, molte altre distribuzioni hanno seguito questa strada catturando molti utenti windows. :-)

Con questo, concludo questo breve articolo sulla regina delle distribuzioni Live, sperando che vi possa essere utile in qualche modo come lo e' stato per me' nel corso di molti anni di assistenze informatiche.

Di nuovo, un saluto a tutti quanti voi e buona navigazione in rete :-)

Sistemi operativi: Backup e ripristino dati con Clonezilla, salviamo i nostri dati in modo professionale e sicuro.

Post n°28 pubblicato il **04 Giugno 2012** da exodus1984
Carissimi bloggers, oggi parliamo di backup e di ripristino dati, ovvero il recupero di dati corrotti e persi usando un sistema OpenSource chiamato Clonezilla.

Questa alternativa libera per il backup/restore dei dati, e' molto piu' valida di altri costosissimi programmi commerciali equivalenti, benche' il software sia in continuo sviluppo e aggiornamento, questa distribuzione molto particolare, ha contribuito a salvare in modo efficace milioni di sistemi operativi che altrimenti sarebbero andati perduti per sempre.

NOTA IMPORTANTE !!!
Leggete con attenzione cio' che segue, prima di attivare il pulsante di autodistruzione sul vostro fidato computer... ;-)))

Prima di iniziare con le spiegazioni tecniche, vorrei dire una cosa semplice a tutti coloro che comprano un computer, portatile o fisso che sia, dopo che il vostro sistema windows si sara' installato all'accensione del dispositivo, prima di fare qualunque altra cosa, effettuate subito un backup dell'immagine originale, perche' se vi dovesse succedere qualcosa come virus, malware, e altre porcherie che prenderete in rete, non avendo il CD di ripristino siete completamente fregati... ;-))(a meno che non passiate a Linux... 8-))

Molte persone che comprano un computer, credono che questo duri in eterno, ma i guai informatici sono sempre dietro l'angolo, pero' tutti se' ne' accorgono sempre troppo tardi, quando non sempre e' possibile fare qualcosa di utile per salvare il loro sistema operativo... :-(
Alcuni clienti che conosco, sono passati a Linux dopo una devastante esperienza di questo tipo, percio' gente, meditate sempre perche' le soluzioni si trovano sempre, ma a volte insegnano vere e proprie lezioni di vita informatica, come in questi casi.

E non fate come certe persone che conosco, che comprano i programmi per il backup solo quando vedono che il loro computer e' ormai un cadavere... :-)
Fare il backup di un'immagine dati ormai corrotta, non serve piu' a nulla, per cui, pensate a fare il backup subito sul vostro nuovo computer, prima di usare sia il sistema che la rete internet. :-)

Bene bene, tuffiamoci come tanti pinguini direttamente sul sito Web di Clonezilla:

http://www.clonezilla.org/downloads/stable/iso-zip-files.php

clonezilla-live-1.2.12-60-amd64.iso
clonezilla-live-1.2.12-60-i486.iso
clonezilla-live-1.2.12-60-i686-pae.iso

Queste immagini sono rispettivamente create per:
32 bit
I486
clonezilla-live-1.2.12-60-i486.iso

32 bit
I686
clonezilla-live-1.2.12-60-i686-pae.iso

64 bit
SMP 64
clonezilla-live-1.2.12-60-amd64.iso

Tutte queste estensioni, vi servono per usare le varie .iso partendo appunto da computer molto vecchi a quelli piu' moderni multiprocessore.

Detto questo, iniziamo a far comprendere questo ambiente ai neofiti del backup e del recupero informativo dopo un disastro informatico.
Clonezilla e' un software in grado di clonare il contenuto del vostro disco fisso o di singole partizioni, creando appunto dei file immagine che possono essere messi al sicuro, usandoli poi come recupero dati

per ripristinare il vostro computer come se fosse nuovo, appena uscito di fabbrica.

Dobbiamo pero' informare tutti gli utenti neofiti che per effettuare un backup, bisogna disporre di un supporto hardware che abbia almeno una capienza uguale o meglio anche superiore al disco fisso che e' montato di default sulla macchina di cui dovremo salvare il sistema operativo che ci interessa.

Durante i miei interventi informatici, ho visto cose davvero strane, per esempio: programmi commerciali a pagamento che si rifiutavano di eseguire il backup di sicurezza da sistemi windows proprietari pur essendo usati come amministrativi, questo perche' era presente un sotto-sistema creato dalla casa di costruzione del computer che ne' impediva l'uso.

Questo fatto, oltre che a far arrabbiare il cliente che giustamente aveva speso dei soldi per comprare un programma di backup, quando finalmente aveva installato il programma, questo non portava a termine il lavoro per cui era stato installato sul sistema.
L'unica scelta possibile in questo caso era sempre evitare il caricamento di windows usando un sistema di recupero LiveCD.

Clonezilla percio', parte al boot del computer come unita' Live, mettendo a disposizione tutti gli strumenti di backup e di ripristino dell'immagine quando si deve assolutamente salvare un determinato sistema operativo.
Questa procedura by-passa di fatto qualsiasi protezione venga creata sul sistema operativo posto sotto backup, rendendo semplicemente inutili tutte le protezioni create per quel determinato sistema.

Backup dei sistemi:
####################

Al boot, sceglieremo l'impostazione della lingua italiana, usando i tasti di direzione e confermando con il tasto invio.
Per il backup del sistema, dovremo scegliere Start_Clonezilla e confermare con invio.
La modalita' "device-image", viene usata quando la partizione deve essere copiata su un file immagine(il nostro caso) oppure scegliete "device-device"
per copiare i dati di una partizione su un'altra.
Quindi dovremo selezionare "localdev" per lavorare sulla partizione locale, e quindi selezioniamo la partizione che ci interessa copiare, infine, dovremo scegliere un percorso valido dove salvare la nostra immagine dati, quindi scegliere la modalita' "beginner" per procedere con la copia.
in seguito, sceglieremo "savedisk" per salvare la nostra immagine sul disco di backup, a questo punto dovremmo dare il nome alla nostra immagine dati che verra' salvata a tutti gli effetti sul supporto di backup prescelto.

Ripristino dei sistemi:
########################

Al boot di Clonezilla, dovremo scegliere sempre la keymap della nostra tastiera(It), in modo da poter lavorare bene durante il recupero del sistema operativo danneggiato.
Dopo avere selezionato la tastiera italiana, selezioneremo sempre Start_Clonezilla, qui, abbiamo due modalita' per il ripristino delle immagini dati sul sistema target: "device to image", che ci servira' per usare l'immagine da copiare per il nuovo sistema operativo, e "device to device", che possiamo usare da partizione a partizione, nel nostro specifico caso, selezioneremo "device to image", e quindi sempre "localdev" per copiare i nuovi dati sul disco locale.
Ora, selezioniamo il disco sorgente, la directory dove abbiamo salvato in precedenza il file immagine del nostro sistema operativo, e quindi utilizziamo la modalita' "expert", e tra le sue opzioni, dovremo selezionare la modalita' "restoredisk" che ci permette appunto di ripristinare il nostro sistema da una immagine dati su disco.
Selezionata l'immagine che ci serve, selezioniamo la partizione o disco che dovra' contenere i dati ripristinati, ora vi verranno richiesti alcuni parametri di configurazione, scegliete "ok" per quelli standard e potrete partire per il vostro recupero totale dei dati corrotti e perduti. :-))

Anche per oggi e' tutto cari bloggers, di nuovo, buona navigazione su internet e buone assistenze informatiche a tutti voi. ;-))

Pensieri e ricordi: il giorno in cui la mia vita e' cambiata.

Post n°29 pubblicato il **07 Giugno 2012** da exodus1984
Carissimi bloggers, oggi e' un giorno molto speciale, per cui, vi raccontero' una parte del mio passato informatico, per ricordare tutte le persone scomparse che hanno fatto di me' quello che sono oggi.

Sono ormai passati quasi 29 anni da allora, e il ricordo di fatti successi e' ancora cosi' reale e vivo come se fosse accaduto soltanto ieri... :-)
Erano gli anni in cui l'italia poteva in qualche modo dare il meglio di se', sia a livello economico che morale, e la mia bella Italia, si apprestava a fare la sua bella figura di fronte a tutto il resto del mondo.

Fu' cosi' che nei primi e ruggenti anni 80', uno sbarbatello entrava in contatto con il settore elettronico e informatico, ma non aveva idea che tutto questo, avrebbe cambiato la sua vita per sempre.
Mi sono sempre chiesto se questo fosse stato il mio destino fin dall'inizio, ma tutt'ora non trovo ancora una valida risposta a questa domanda... :-))

Ho lavorato per tutto il 1983 alla costruzione di circuiti di memoria, finche' nel dicembre dello stesso anno, venne a trovarmi una persona molto particolare che mi invito' a svolgere alcuni test elettronici ed informatici presso la sua sede, con l'obiettivo di creare un programma di cifratura che potesse proteggere la sua azienda dalle continue fughe di informazioni industriali e tecnologiche che erano molto avanzate per l'epoca.

E' stato cosi' che mi sono ritrovato immerso in un mondo tutto nuovo e per l'epoca, molto strano per tutte le persone che non ne' erano a conoscenza.
Infatti, parlare di computer nel 1983, era quasi considerato eretico per l'economia locale, e, almeno nella mia zona di residenza, era qualcosa che andava oltre la comprensione della ragione umana... :-)

Se si parlava di computer, e di periferiche, molta gente non sapeva di che cosa si stava parlando, e quindi come di consueto, cercavano di evitare l'argomento solo perche' non conoscevano bene la materia.
Nel corso di tutti questi anni, ho visto cose stupende e incredibili che per la maggior parte della gente comune, molto probabilmente, non potra' mai vedere.

Ma ritorniamo alla giornata dei ricordi, i ricordi di tante persone che purtroppo oggi non ci sono piu', gente che ha fatto di me' una persona nuova e forse, per qualcuno, anche migliore di quello che ero e che sono stato durante tutti questi anni.
A tutti loro, devo l'onore e il rispetto che mi e' stato insegnato, a loro devo la mia vita e quello che sono diventato oggi, e continuero' cosi' finche' la mia vita me lo permettera'.

In tutti questi lunghi anni, ho fatto cose che la gente comune, non fara' mai, negli anni a seguire il 1983, dopo il mio primo incontro con questo vecchio signore, ne' segui' un altro, e poi un altro ancora, finche' un giorno di giugno del 1984, ci ritrovammo tutti quanti a Udine in un luogo che per me' aveva dell'incredibile : computer, computer e ancora computer, ma ancora non avevo visto tutto...:-)

Avevo 17 anni quando la mia vita prese una strada diversa da quella che svolgevano tutti i ragazzi della mia eta', loro avevano la scuola, i divertimenti e le vacanze in estate, io scelsi invece di rinunciare a tutto questo per una causa in cui credo ancora oggi, e per la quale tante persone
hanno contribuito, facendomi capire che l'onore, il rispetto, la conoscenza e la lealta', vanno di pari passo con la nostra vita, e che quindi dobbiamo seguire questi semplici accorgimenti per avere una vita da vivere completamente nuova.

Tutto quello che ho imparato, lo devo a queste persone, perche' loro mi hanno insegnato cose che non si imparano a scuola, ho sostenuto diversi esami interni da quando ho fatto la mia scelta di vita, e non mi sono mai voltato indietro.
Mentre tutti i miei amici di allora si divertivano, io studiavo i sistemi informatici, costruivo programmi speciali per i computer, lavoravo con le informazioni, studiavo la nuova conoscenza informatica, costruivo i computer e manipolavo le reti di tutto il mondo.

Di tutte le persone invitate a Udine in quel lontano giorno di giugno del 1984, ne' furono scelte solamente due, una di queste ero io e a 17 anni, potete solo immaginare come vi sareste sentiti, poter lavorare per queste persone, imparando tantissime cose che altrimenti non avrei mai potuto imparare per via della mia bassa estrazione sociale(famiglia povera).

Da allora, sono successe moltissime cose, ma la scomparsa dei miei amici conosciuti durante l'addestramento informatico, non ha cambiato il mio destino, mi ha reso piu' forte e ancora piu'

determinato a proseguire su questa strada, come mi e' stato insegnato.

Pensando all'Italia di oggi e a quella che era un tempo, vedo che bisognerebbe cambiare le cose, anche perche' i valori che mi sono stati insegnati come onore, rispetto, lealta', e spirito di sacrificio, oggi non sono piu' condivisi dalla gente, e forse anche per questo l'italia e' cambiata in peggio.
Potra' sembrare banale a molti di voi, ma io che mi ritengo un buon cittadino italiano, e sono anche molto patriottico, credo fermamente in questi insegnamenti, perche' sono stati davvero la mia fortuna cambiando la mia vita per sempre.

La mia bella Italia, sempre maltrattata da tutti quanti, ma non da me'.
Questo, puo' essere ancora un grande paese, ma il governo deve impegnarsi davvero e scegliere i cambiamenti che vanno fatti, non solo quelli che vanno bene ai partiti politici del momento.

Al governo posso dare un consiglio: trattatemi bene l'Italia.
Ai politici invece darei in mano una zappa e li manderei a lavorare sotto il sole di mezzogiorno, cosi' vedono la fatica che si fa' per portarsi a casa il pane...:-)

Tutti i governi sanno mettere le mani nelle tasche dei cittadini, ma i veri cambiamenti, non si fanno mai perche' le cose vanno bene cosi'per loro, intendo... :-)
Non ce' onore in quello che il governo sta' facendo all'Italia, non ce' rispetto per i cittadini, e lo spirito di sacrificio, lo devono avere sempre e solo quei poveri diavoli che devono pagare ogni nuova tassa imposta, mentre i politici se la ridono...:-(
Quello che mi e' stato insegnato, la mia etica professionale, e tutto il resto, mi hanno permesso di fare molte cose, e forse anche di piu'...

Questo e' un breve estratto della mia vita, chi mi conosce, sa' bene cosa sto' dicendo, mentre i bloggers, possono solo tentare di capire la mia particolare situazione. :-)

Cari bloggers, anche per oggi e' tutto, di nuovo buona navigazione e buon divertimento su internet a tutti voi :-)

Analisi matematiche: teoria e previsione dei numeri al Superenalotto.

Post n°30 pubblicato il **09 Giugno 2012** da exodus1984
Carissimi bloggers, oggi parliamo di Superenalotto, chi di voi non ha mai provato a giocarci? :-))

Questo gioco, offre molti spunti a livello matematico, sia per la previsione dei numeri che per la possibilita' di creare funzioni matematiche particolari che possano darci un'idea di come e quando giocare una serie di numeri che riteniamo utili e vincenti.

Oggi analizziamo questi aspetti matematici per capire e creare una equazione parametrica che ci permetta di giocare e poter vincere qualcosa di utile in termini di denaro... ;-))

Benche' il denaro non sia la mia priorita' principale, vincere un premio in denaro che proviene da un gioco calcolato e guidato da una funzione matematica, mi da' sempre una grande soddisfazione, che non e' quella di avere fisicamente il denaro della vincita, ma e' la soddisfazione di poter sapere che i numeri da noi calcolati, erano previsti per l'estrazione corrente.

Andiamo ad iniziare:

Definiamo RM come valore costante che ci permette di sapere quante volte dovremmo giocare una colonna diversa prima di acchiappare un sei(6).

Definiamo GB come valore della singola colonna.

Definiamo CRS come valore del singolo concorso di una giocata a settimana.

Definiamo 3CRS come valore dei tre concorsi a settimana.

Ed ecco qui come procedere:

$$\frac{(RM) / 2 * (RM) / 365 / \{GB\}}{_____} = [CRS\text{-}RM\text{-}GB]$$

(CRS = RM / {GB}) = CRS * 3)

Detto questo, dovremo precisare che per una giocata a settimana, avremo a disposizione solo 1705793.507 possibilita' di fare un risultato utile, e qui parliamo di prendere il tre(3) e il quattro(4), mentre le possibilita' di fare un cinque(5) o un sei(6) aumentano esponenzialmente ad ogni giocata, rendendo la complessita' di calcolo una vera e propria sfida per le menti matematiche che teorizzano una sequenza di numeri validi in successione costante e prevedibile.

La bellezza di questo gioco, almeno per me', e' solamente a livello di calcolo, ma considerando che almeno il tre(3) e' abbastanza prevedibile, con una cadenza di circa 1-2 volte alla settimana, la bonta' di questi calcoli, rivelano che siamo sulla strada giusta per arrivare al sei(6), benche' di fatto, non sia possibile se non tramite una riduzione matematica dell'unica possibilita' reale ad una cadenza prefissata ogni 622614630 volte, in cui bisognerebbe giocare tutti i numeri presenti(1-90), e questo vorrebbe dire che per esempio, per prendere un sei(6) da circa 62 milioni di euro, dovremmo investire circa 10 volte questa cifra per avere "solo" un premio di 62 milioni di euro... ;-))

Il calcolo di nuovi sistemi matematici in grado di avvicinarsi al sei(6)
e' tuttavia molto affascinante, ogni calcolo puo' ritrovare la nuova combinazione vincente, e questo, e' solo un semplice tentativo di usare dei numeri per trovare altri numeri.

Se volete provare a giocare, vi mando i numeri estratti dal programma che usa questa formula matematica appena descritta, e si riferisce all'ultimo concorso del 07-06-2012, giocabile per la sola giornata di oggi.

Calcolo Jolly(previsto) : 21

30 56 61 66 73 76	2
26 52 57 62 69 72	1
20 46 51 56 63 66	1
12 38 43 48 55 58	1
1 25 30 35 42 45	1
1 13 18 23 30 33	1

12 17 22 29 32 1
9 14 19 26 29 1
4 9 14 21 24 1
1 2 7 14 17 1
1 1 1 5 8 1
1 1 1 1 1 1

Questo calcolo matematico, non tiene conto del numero 1, che nonostante sia perfettamente giocabile, in questo caso non assume una rilevanza necessaria, i numeri in gioco sono solo quelli oltre il numero 1, la previsione del numero jolly viene fatta tramite lo stesso metodo indicato nell'equazione precedente. Come potete osservare, togliendo tutti i numeri uno(1), rimangono i possibili numeri previsti per l'estrazione di oggi, sabato 9 giugno 2012.

E anche per oggi e' tutto cari bloggers, un saluto a tutti voi e buona fortuna per l'estrazione di questa sera ;-))

Riflessioni personali su Internet: l'etica hacker nel moderno mondo virtuale.

Post n°31 pubblicato il **10 Giugno 2012** da exodus1984
Carissimi bloggers, oggi parliamo di etica, una cosa che non tutti possiedono purtroppo... e questo, lo ritroviamo ogni giorno in tutto quello che ci circonda, siti web, messaggi e-mail e molto altro... :-)

Un argomento che mi piace e' essenzialmente il continuo susseguirsi di eventi informatici strani ed affascinanti, nei quali si puo' ritrovare l'etica particolare del comportamento umano in vari settori applicativi e sempre piu' tecnologici.

Per questo, affrontare un argomento come l'etica hacker e' forse un po' azzardato, in quanto gli hacker stessi sono maltrattati da tutti, stampa compresa, per non parlare dei guai che derivano da un'etica che non ha fondamenti specifici, ovvero: posso bucare un server per far valere le mie ragioni? Che etica mi dovrei imporre per non toccare la liberta' degli altri?

Essenzialmente, tralasciando che ci sono leggi ben precise sulle intrusioni informatiche non autorizzate, l'etica hacker non e' uguale per tutti i soggetti presi in esame, alcuni lo fanno per noia, alcuni lo fanno per soldi, altri invece, lo fanno per una causa in cui credono, senza nessun tornaconto di carattere economico.

Alcuni ideali che hanno fatto muovere gli hacker, sono essenzialmente la liberta' di informazione, la privacy, e la censura che impedisce il libero scambio di informazioni (conoscere alcune verita' puo' essere pericoloso...).

Tutti i governi del pianeta hanno avuto a che vedere con diversi gruppi hacker, e per questo cercano di "mantenere il controllo" della rete internet formando dei reparti speciali telematici che tengono sotto controllo quello che interessa loro o le relative persone fisiche poste sotto controllo per qualche motivo o indagine in corso.

Ci sono sistemi automatici che riconoscono e leggono i messaggi di posta elettronica alla ricerca di informazioni particolari, prima ancora che voi possiate aprire il messaggio in questione, quindi se potete farlo, cifrate sempre la vostra posta elettronica, renderete piu' difficile la vita a tutti questi sistemi di spionaggio che sono messi li' con uno scopo ben preciso, controllare prima le vostre abitudini, e poi il vostro stesso pensiero, e questo non e' uno scherzo quando si tratta della vostra liberta' individuale sulla rete internet... :-)

Nel 1996, il parlamento europeo scopri' "per caso" l'esistenza di un sistema di intercettazione a livello mondiale per il controllo dei cittadini in Europa e in molte altre nazioni del mondo, che operava su tutte le reti disponibili(telefoni, cellulari,internet,tv etc. etc.),allora si parlava di circa 300 milioni di intercettazioni in corso ogni giorno, per 365 giorni l'anno, moltiplicate per circa una ventina d'anni d'uso del suddetto sistema... :-)

L'etica hacker prende in considerazione tutti questi aspetti che riguardano la liberta' di rete e la liberta' individuale di ogni persona connessa attraverso la rete, e per farlo, vengono attaccati i server di tutto il mondo, solo per poter reclamare il proprio diritto ad esistere e vivere liberi sulla grande rete.

Ma l'etica, non si ferma qui, l'etica e' una cosa che ciascun hacker si deve imporre, nel bene e nel male. I governi temono gli hacker, e li temono perche' proprio in molti casi pubblici, gli hacker raccontano le verita' nascoste ai cittadini dai governi stessi, ed e' cosi' infatti che gli hacker finiscono braccati e maltrattati dalla stampa e dai governi di tutto il pianeta.

Tutto questo, forma la grande rete, i governi da una parte che cercano di controllare il pensiero dei cittadini, gli hacker dall'altra che cercano di mantenere i loro diritti e la liberta' di rete.
Nonostante questa continua guerra informatica, in cui non si capisce bene chi sia il buono e chi sia il cattivo di turno, proprio per via dell'etica, un hacker puo' essere considerato buono o cattivo allo stesso tempo, ed e' solo a lui che spetta la decisione finale da prendere durante un assalto informatico programmato.

Naturalmente, l'etica hacker e' molto piu' di quello che ho scritto in questo articolo, pertanto vi invito tutti quanti a leggere in rete tutto quello che trovate al riguardo, cosi' potete farvi un'opinione personale e senza censure di quello che ho scritto qui.

In ogni caso, l'etica hacker, deve nascere dall'interno di ogni singolo individuo informatico, dopo che naturalmente avra' fatto le sue esperienze in ogni campo in cui desidera imparare qualcosa, inoltre, il senso di responsabilita' insito in ciascuna persona, deve prevalere sul bene e sul male che un hacker puo' provare in ogni determinato momento della propria vita.

Cosi', tutti possiamo essere hacker, anche senza saperlo, ma in pratica non lo saremo mai, questo perche' la conoscenza e' un fattore matematico infinito che ci porta a scoprire e imparare sempre cose nuove, e considerando che nella vita abbiamo sempre qualcosa da imparare, questo fa si' che un hacker non sia mai veramente un vero hacker se non potra' avvalersi di un'etica valida per mantenere la sua liberta' e quella degli altri.

La condivisione delle informazioni, fa' parte dell'etica hacker, anche se per molto tempo si e' dibattuto se certe informazioni debbano essere davvero divulgate, ma gli hacker esistono per questo, la conoscenza deve essere condivisa con tutti, e non deve far parte solo di una ristretta cerchia di personaggi che si credono Dio...(governi e simili) :-)

Un hacker puo' dare e puo' togliere alla rete tutto cio' che vuole, e questo in barba ai controlli dei governi di tutto il pianeta, ma una cosa sola lo separa da Dio, ovvero: la sua etica personale, imposta e creata appunto per
rendere di nuovo giustizia alla grande rete e a tutte le persone che la popolano.

Ce' stato un tempo in cui anche io ero prigioniero di una ristretta cerchia di persone, e mi credevo un Dio in terra, per quello che facevo, per quello
che riuscivo a fare agli altri, potevo fare tutto quello che volevo, e i limiti venivano sempre infranti senza nessuna esclusione di colpi, poi, un giorno di tanti anni fa', una persona speciale mi mostro' la strada giusta, la strada che percorro ancora oggi.
Oggi quella persona e' scomparsa, ma quello che mi ha lasciato, e' qualcosa di grande, di un valore infinito per il quale, non potro' mai ripagarla abbastanza, infatti, molte volte, non capivo se ero io a cercarmi i guai oppure se erano i guai a trovare me'... :-)

Percio' cari bloggers, l'etica non e' solo hacker, ma ci serve nella vita di tutti i giorni per vivere e condividere le nostre esperienze personali con le persone con cui entriamo in contatto, perche' condividere qualcosa con gli altri a volte, evita loro di fare la nostra stessa fine, quindi, ricordate bene che non ci potra' essere sempre una persona speciale che vi togliera' dai guai ogni volta che ci finite dentro... :-)

Con questo concludo subito l'articolo senza dilungarmi troppo, altrimenti di questo passo, potrei arrivare anche a scrivere un nuovo libro sugli hacker e la rete... ;-) (ACDL 2.0???) :-)

Di nuovo a tutti voi cari bloggers, buona navigazione e buon divertimento in rete :-)

Sistemi operativi: la stupenda distribuzione PartedMagic usata nelle assistenze informatiche.

Post n°32 pubblicato il **11 Giugno 2012** da exodus1984
Carissimi bloggers, oggi parleremo di una distribuzione Linux-Live in grado di aiutarci a ridimensionare il nostro disco fisso, ad avere accesso al nostro sistema windows(XP/Vista/7???) manipolando gli account utente e/o cancellando le password amministrative per ottenere un libero accesso al sistema in modo da recuperare i files che ci interessano salvando il nostro lavoro.

Questa piccola meraviglia della tecnica informatica moderna, si chiama appunto PartedMagic, ed e' un sistema creato per il recupero di partizioni, spostamento dati e ridimensionamento del disco fisso di ogni computer, ma allo stesso tempo, e' anche un validissimo sistema operativo che ci mette a disposizione diversi programmi molto utili durante le nostre assistenze informatiche.

Andiamo subito a visitare il sito della distribuzione:

http://partedmagic.com/doku.php?id=downloads

Qui, troviamo tre tipi di file .iso masterizzabili a seconda del sistema su cui dovrete operare:

pmagic_2012_06_07.iso (md5sum: 42467de365131406f0ae1ba0af23f7dd)

pmagic_2012_06_07_i486.iso (md5sum: 43c7058e7ae38e177bc39befd38293b7)

pmagic_2012_06_07_x86_64.iso (md5sum: 3ff60be3f11a6646e3f939b7fe607bb5)

Copiate il file .iso che vi interessa sotto una directory di test, e prima di masterizzarlo, testate la somma MD5 (Message Digest algorithm 5), che vi dice in parole povere, se il file .iso e' scaricato correttamente oppure ha subìto corruzioni durante il trasferimento internet.

In pratica, la somma MD5 garantisce l'autenticita' di un qualsiasi file che non ha subìto modifiche dalla sua creazione, MD5 restituisce una firma elettronica perche' gli utenti sappiano che la loro copia del file, e' originale e non contraffatta. :-)

Il comando Linux per sapere che il cd masterizzato sara' originale e' questo:

parsec@exodus84:~$ md5sum pmagic_2012_06_07.iso

e quindi premete invio per confermare, il risultato dovrebbe essere uguale alla firma originale presente sul sito web del produttore:
md5sum: 42467de365131406f0ae1ba0af23f7dd

Se il risultato di questa operazione sara' perfettamente uguale alla somma MD5 presente sul sito del produttore:
md5sum: 42467de365131406f0ae1ba0af23f7dd

allora, e solo se perfettamente identica all'originale, potete masterizzare il cdrom senza problemi, al contrario, se la somma MD5 e' diversa da quella del produttore originale del file .iso, non masterizzate il cdrom perche' il risultato e' certamente un file .iso corrotto durante il trasferimento su internet, e questo puo' succedere per vari motivi di rete, ma anche se qualcuno intercetta il nostro trasferimento di dati e vi inietta una manciata di pacchetti malefici, atti a deturpare il suddetto file .iso :-)
(conosco molti tapiri di rete che lo fanno 24 ore al giorno...:-)))

Su sistemi windows, potete usare MD5summer, oppure altre utility di questo tipo per verificare che la firma digitale di un programma corrisponda sempre all'originale distribuita dal produttore.

Dopo che avrete letto le Faq sul sito, e un minimo di documentazione tecnica, potrete utilizzare al meglio questa piccola distribuzione per il recupero dati dai vostri sistemi windows.
Scaricate quindi il file che vi interessa per la vostra macchina, e procedete alla masterizzazione.

Sul sito trovate anche una breve descrizione di come rimuovere le password dai vostri sistemi Windows, usando il comando Linux "chntpw", questo comando, accede fisicamente al file SAM di windows in cui sono conservate informazioni cifrate relative agli utenti disponibili su quel determinato sistema windows.

L'utilizzo di chntpw, viene richiesto quando sussiste la necessita' di forzare l'account di amministratore

per il sistema windows quando ci si dimentica la password, oppure come utente senza privilegi per avere accesso al proprio account.
Negli ambienti investigativi, e' procedura comune copiare il file SAM originale del sistema Windows, mettendolo da parte e cancellando le password sul file locale, questo succede quando si vuole avere accesso ad un pc windows, per controllare se la moglie o il marito, si tradiscono, ripristinando poi il file originale con le sue password autentiche in modo che nessuno possa sospettare dell'avvenuta intrusione sul computer usato in casa dai coniugi...:-)

In molti casi di computer forensic, viene spesso utilizzato quando il colpevole non fornisce le password di autenticazione, ma di solito, una buona distribuzione live che implementi il driver ntfs-3g, e' piu' che sufficiente per recuperare informazioni da un sistema windows posto sotto indagine informatica, naturalmente sempre che non risulti cifrato una volta aperto il disco fisso, ma di questo, parleremo in un altro articolo, riguardante la cifratura dei dati personali su sistemi Linux e Windows. :-)

Per poter usare chntpw, e' necessario montare prima il disco fisso su cui e' installato il vostro sistema windows, per farlo, usate il comando mount di Linux, oppure il driver diretto ntfs-3g che puo' leggere e scrivere dati da e verso partizioni windows formattate appunto con filesystem di tipo ntfs.

Ecco un semplice esempio d'uso di chntpw per il login senza password su Windows Vista dopo che il relativo disco fisso contenente il sistema operativo MS e' stato montato usando un bay esterno per il backup:

##

```
root@PartedMagic:~# chntpw /media/sdb1/Windows/System32/config/SAM
chntpw version 0.99.6 110511 , (c) Petter N Hagen

Hive name (from header):

ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c
File size 262144 [40000] bytes, containing 7 pages (+ 1 headerpage)
Used for data: 246/52976 blocks/bytes, unused: 21/8240 blocks/bytes.

* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length        : 0
Password history count         : 0
| RID -|---------- Username ------------| Admin? |- Lock? --|
| 01f4 | Administrator                  | ADMIN  | dis/lock |
| 03e8 | exodus1984                     | ADMIN  |          |
| 01f5 | Guest                          |        | dis/lock |

----------------------> SYSKEY CHECK <-----------------------
SYSTEM   SecureBoot           : -1 -> Not Set (not installed, good!)
SAM      AccountF             : 0 -> off
SECURITY PolSecretEncryptionKey: -1 -> Not Set (OK if this is NT4)
Syskey not installed!

RID     : 0500 [01f4]
Username: Administrator
fullname:
comment : Account predefinito per l'amministrazione del computer/dominio
homedir :

User is member of 1 groups:
00000220 = Administrators (which has 2 members)

Account bits: 0x0211 =
[X] Disabled        | [ ] Homedir req.    | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout    | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |
```

Failed login count: 0, while max tries is: 0
Total login count: 1

- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vista)
 3 - Promote user (make user an administrator)
 4 - Unlock and enable user account [probably locked now]
 q - Quit editing user, back to user select

Select: [q] > 1 <-cancelliamo la password e facciamo il login con invio

Password cleared!

Hives that have changed:
 # Name
 0
Write hive files? (y/n) [n] : y
 0 - OK
root@PartedMagic:~#

##

Se avete necessita' particolari o vi siete portati a casa il disco fisso del cliente, allora potete usare il vostro sistema Linux per il recupero, collegando il disco fisso ad un dock multifunzione che ha appunto lo scopo preciso di connettere i vari dischi fissi al vostro computer usando una connessione veloce usb 2/3. Il disco del cliente, verra' montato in sola lettura, questo per proteggere i dati proprietari da una cancellazione accidentale, ma se il cliente da' il suo consenso oppure i dati non sono molto importanti, si puo' optare per una lettura diretta avendo a disposizione anche la scrittura sul dispositivo, in modo che sia possibile anche cancellare i files richiesti dal cliente, ricordate pero' che prima bisogna sempre chiedere al cliente che cosa vuole fare dei dati in suo possesso, in modo che si possa impostare una procedura di recupero/formattazione completa senza arrecare danno al cliente stesso.

Su internet, potete trovare delle docking station con bay per hard disk di vari formati e di varie specifiche di connessione ad un prezzo molto basso, quindi guardate le etichette dei dischi per sapere il tipo di supporto che avete sottomano: ata, sata e-sata,sata 2, 3, etc.etc. :-)

A questo punto, il vostro sistema Linux di recupero, avra' gia' montato il disco fisso via usb, e potete usare il semplice copia-incolla per i files tra un disco e l'altro, oppure scegliere se lanciare l'applicazione Gparted se dovete effettuare un backup di partizione, oppure la clonazione dell'intero disco(partizioni diverse su supporti diversi) usando Clonezilla che e' integrato su questa piccola distribuzione Linux.

E con questo cari bloggers, un saluto a tutti voi, augurandovi buona permanenza in rete, e di nuovo, buon divertimento :-)

Sistemi Windows: velocizzare il sistema su internet e in locale con CCleaner

Post n°33 pubblicato il **15 Giugno 2012** da exodus1984
Carissimi bloggers, oggi tratteremo alcuni programmi per la manutenzione dei sistemi Windows.

Iniziamo subito con quello forse piu' conosciuto, che ci permette di riportare il nostro sistema Windows alla sua velocita' di origine, ripulendo files, e risistemando il registro di sistema.
Il programma in questione e' il famoso CCleaner, che ci puo' aiutare davvero molto in parecchie assistenze informatiche in cui il sistema windows installato, risulta lento e con una scarsa risposta internet nel caricamento delle pagine web.

Detto questo, andiamo subito al sito del produttore:

http://www.piriform.com/ccleaner/download

Qui, scegliete la versione free, e scaricatela cliccando sui link sottostanti.
Il file scaricato, avra' un nome del tipo "ccsetup319.exe", localizzate il file sul vostro sistema e iniziate l'installazione.

Quando installate il programma, fate attenzione a scegliere la vostra lingua, nel nostro caso l'italiano.
In seguito dopo che avrete accettato i termini della licenza, il setup terminera' lanciando subito il programma e quindi sarete pronti a far correre di nuovo il vostro esausto sistema Windows.

Sul pannello principale di CCleaner, verranno utilizzati solo i primi due strumenti, ovvero il pulsante con la scopa dove viene indicato il testo "Pulizia":

1) cliccare il pulsante "Analizza", e quando l'analisi sara' terminata, cliccare sul pulsante "Avvia Pulizia", verrete informati che il processo eliminera' definitivamente i files analizzati precedentemente.
Cliccate su OK per confermare e avrete terminato la prima parte del ripristino di sistema.

2) cliccare il pulsante "Registro", quindi cliccare il pulsante della scheda "Trova Problemi" e verra' avviata un'analisi completa come per la precedente funzione di pulizia.
Appena sara' terminata questa nuova analisi, cliccate sul pulsante "Ripara selezionati", e quando vi compare la finestra del backup, potete cliccare su "No" se non volete salvare i valori e quindi procedete alla prossima fase.

A questo punto, vi compare una nuova finestra nella quale potrete riparare un solo file oppure ripararli tutti, selezionate il pulsante "Ripara Selezionati" e quindi avrete terminato.

Devo dire che nella maggior parte dei casi da me' trattati con questo programma, ho ottenuto risultati davvero sorprendenti in termini di velocita' e di risposta del sistema Windows posto sotto assistenza. :-)

Gli altri due pulsanti della scheda principale di CCleaner, "Strumenti" e "Opzioni" non sono stati usati durante le sessioni di ripristino dei sistemi, in quanto la sistemazione del registro e la pulizia dei files hanno garantito una nuova vita per per le macchine in assistenza.

Le configurazioni che si possono fare sono davvero molte, ma per un'assistenza informatica veloce e stabile, questo programma e' davvero utile per rimettere "in sella" il sistema windows e farlo correre di nuovo su internet e a livello locale.

Per oggi e' tutto cari bloggers, un saluto a tutti voi e un augurio di buona permanenza su internet. :-)

Sistemi Windows: manutenzione del disco rigido con UltraDefrag

Post n°34 pubblicato il **16 Giugno 2012** da exodus1984
Carissimi bloggers, oggi continueremo a trattare le utility per ottimizzare il nostro sistema Windows.
In particolare oggi tratteremo l'uso del programma UltraDefrag per rendere un pochino piu' veloce la gestione del nostro disco NTFS e di conseguenza, la risposta applicativa di tutto il sistema installato.

Come sempre, andiamo direttamente al sito del produttore per il consueto download:

http://ultradefrag.sourceforge.net/en/index.html?download

Qui sul sito, troveremo tre diverse build del programma per i rispettivi ambienti operativi:

Download UltraDefrag 32bit/64bit/Itanium

32-bit Windows
NT4.0, 2000, XP, Vista, 7 - Server NT4.0, 2000, 2003, 2008

64-bit Windows
x64 Editions of XP, Vista, 7 - Server 2003, 2008, 2008 R2

64-bit Windows running on Intel Itanium processor

Normalmente, per gli utenti standard, le versioni 32 e 64 bit per windows sono quelle piu' utilizzate nel parco macchine basate su sistemi windows per utenti domestici e workstation.

Scarichiamo come sempre il file che sara' piu' adatto alla nostra tipologia di processore e procediamo con il setup di installazione.
La finestra di benvenuto, vi invitera' a cliccare sul pulsante "Next", quindi dovrete dare un'occhiata alla licenza GNU e cliccare sul pulsante "I Agree".

La finestra che vi compare adesso, vi invita a controllare i componenti che volete avere dopo l'installazione di UltraDefrag.
Cliccate nuovamente sul pulsante "Next" e procedete con la scelta della lingua di destinazione, nel nostro caso, la lingua italiana. :-)

Quando avrete scelto la lingua di destinazione, cliccate sul pulsante "Install" e i wizard completera' l'installazione per voi, cliccate sul pulsante "Finish" per terminare e sarete pronti per la vostra prima Ultradeframmentazione del disco.

Dovrete selezionare il disco di destinazione (C: D:), quindi cliccare il pulsante di analisi del disco fisso.
Al termine di questa analisi, vi verranno mostrati la quantita' di dati frammentati che sara' possibile ripristinare per dare al vostro computer windows ancora un sacco di velocita' nell'esecuzione dei programmi e nella presentazione delle interfacce grafiche.

Nella schermata principale di UltraDefrag versione 5.05, cliccate su "Azione", verra' aperto un menu' dove potrete procedere alla deframmentazione del disco.

Selezionare quindi "Analizza"(F5) per procedere con l'analisi del supporto hardware.
Quando la procedura saa' terminata, vi apparira' lo stato di frammentazione del vostro disco fisso, se avete del tempo, potete eseguire la deframmentazione quando non usate il computer, perche' vi porta via parecchio tempo, quindi non e' consigliata mentre lavorate.

La deframmentazione di filesystem Windows, dovrebbe essere fatta regolarmente almeno una(1) volta a settimana, questo vi permette di mantenere un rapporto tra uso e velocita' di sistema molto ottimale, i dischi che hanno maggiormente bisogno di essere deframmentati sono quelli ad alto contenuto di video, musica immagini grafiche e su quei sistemi in genere su cui si lavora parecchio alla modifica di formati video,audio, grafica in generale.

Inoltre, sarebbe consigliata la disabilitazione temporanea del proprio antivirus, solo mentre fate la deframmentazione, perche' questo rallenterebbe di conseguenza tutte le operazioni in corso sul computer.

NOTA IMPORTANTE !!!

####################
Facciamo notare che la deframmentazione, non e' consigliata per le chiavette usb e i nuovi dischi rigidi in tecnologia SSD, in quanto questi supporti verrebbero resi inoperativi entro breve tempo per via della loro struttura interna che non contiene parti meccaniche come i dischi fissi standard, la scrittura e la lettura di questi supporti, e' diversa dai normali dischi meccanici, perche' proprio la scrittura fisica su questi supporti e' limitata nel tempo, e le continue deframmentazioni, renderebbero il supporto Flash/SSD sempre operativo, ma con uno spazio dati interno pari a zero, questo perche' la vita operativa di questi supporti e' data dai cicli di scrittura che diminuiscono progressivamente ed inesorabilmente lo spazio di memorizzazione dati del supporto stesso, cosa che con i dischi meccanici non succede.

Controlliamo quindi la consistenza dei dati sul nostro supporto fisso, dal menu' di windows aprite un terminale cliccando su "Esegui" e digitando il comando "cmd".
Non appena avrete aperto il vostro terminale su Windows, controllerete subito il disco:

c:> CHKDSK c: /F /V

Questo comando vi permette di valutare e fare un controllo prima dell'avvio del sistema operativo per controllare la consistenza dei vostri dati.

Quindi eseguite il comando:

c:> CHKDSK c: /R /F /V

Questo comando controlla il disco e ripara gli eventuali errori, per dare migliore velocita' al vostro sistema windows.

Le utility CCleaner e UltraDefrag, vi permettono di ottenere piu' velocita' applicativa, una migliore velocita' di caricamento delle pagine web, e una gestione del disco fisso davvero impeccabile, infatti, questi due semplici programmi, mi hanno permesso di risolvere il 90% dei problemi che affliggono i sistemi windows, rendendo di nuovo operative migliaia di macchine che montavano questo sistema di default. :-)

Gli utenti windows, in ogni caso, non sempre fanno una regolare manutenzione al loro sistema, e quando i computer arrivano in assistenza, se' ne' vedono di tutti i colori, e anche in bianco e nero... ;-))

Per cui, un consiglio che posso dare a tutti gli utenti windows che non conoscono queste procedure e non sono tecnici e' questo:
avete a disposizione due programmi utilissimi, imparate ad usarli ma soprattutto usateli!!! :-)

Cercate di programmare un periodo di tempo in cui non usate il computer o non vi collegate a internet per fare una manutenzione del disco e ottimizzare il vostro windows, quindi: grafica, audio, video almeno una volta a settimana, per tutto il resto, quando potete nel limite di almeno una volta al mese. ;-))

Cari bloggers, vi ho prescritto la ricetta medica per il vostro computer, e anche per oggi e' tutto, buona navigazione a tutti voi. :-))

Recupero dati: da Linux a Windows con Ext2Fsd

Post n°35 pubblicato il **17 Giugno 2012** da exodus1984
Carissimi bloggers, oggi continueremo con la selezione del software per Windows che ci permette di scrivere e copiare i nostri documenti Windows su un filesystem ext2/4/4 di Linux e viceversa.

Questo driver, si integra benissimo in Esplora Risorse, e riconosce i filesystem Linux montandoli sul supporto principale (C:>) assegnando una lettera per il drive appena montato in modo che possiate leggere il contenuto del disco Linux sul vostro sistema operativo Windows.
Prima di proseguire, visitiamo il sito dell'autore:

http://www.ext2fsd.com/?page_id=7

Questa particolarita' offerta dal driver Ext2FSD, ci permette di recuperare di fatto i dati presenti su un disco partizionato ext2/ext3/ext4 da Linux, attraverso il sistema Windows.
Questo driver, viene usato per "spiare" letteralmente i dati contenuti sulle partizioni Linux e recuperare fisicamente i dati presenti sul supporto, copiandoli attraverso un sistema Windows.

Come sempre, andiamo a scaricare subito il nostro driver dal sito del produttore:

http://sourceforge.net/projects/ext2fsd/files/Ext2fsd/0.51/

Su questa pagina, cliccate sul file eseguibile Ext2Fsd-0.51.exe per scaricarlo.
Ext2Fsd-0.51.exe, e' un file setup di windows, e pertanto, richiede privilegi amministrativi per la sua installazione sul sistema che verra' usato per recuperare dati da Linux.

Durante il setup, vi verranno richiesti alcuni parametri, come directory di installazione e altre cose di questo tipo, cliccate sempre sulle opzioni consigliate dal programma di installazione, ma fate attenzione quando vi chiede la modalita' in scrittura sul filesystem Linux, dovrete abilitare tutte e tre(3) le caselle di scelta e confermare l'installazione.

Adesso, ad ogni login sul vostro sistema windows, vi verra' richiesto il permesso di accedere direttamente al filesystem, confermate sempre perche' altrimenti il programma si ferma e non puo' essere usato.

I permessi amministrativi che il programma vi chiede ogni volta che dovrete recuperare dati da Linux, sono validi solo per quella sessione, il programma ext2mgr.exe vi chiedera' sempre i permessi prima di poter essere eseguito, una forma di cortesia informatica rivolta all'utente. ;-))

I sistemi supportati sono i seguenti:
Windows 2000, xp, 2003, Vista, Win7 (X86, AMD64)

Seguite dunque le FAQ sul sito dell'autore in caso di problemi, ma se siete sviluppatori, potrete crearvi un driver personale che possa funzionare bene su qualsiasi sistema windows, ecco alcuni link utili:

Scaricate il WDK(Windows Driver Kit), che serve appunto per compilare il driver per il kernel di Windows:

http://connect.microsoft.com

Scaricate quindi i sorgenti da questo link e proseguite:

http://ext2fsd.git.sourceforge.net/git/gitweb.cgi?p=ext2fsd/ext2fsd;a=summary

Nella prima configurazione di Ext2Fsd-0.51.exe, potete scegliere alcuni parametri per i dischi che verranno montati sul vostro sistema di recupero dati Windows, se non conoscete bene il significato di alcune definizioni, accettate quelle di default per ora, poi potrete tornare con comodo sulle opzioni ed apportare tutte le modifiche che ritenete necessarie per il vostro lavoro di recupero. :-)

Quando avrete apportato queste modifiche, ad esempio assegnare ad un DEV Linux una lettera di identificazione(E:> F:> etc..), il volume ext3 di Linux verra' montato ogni volta che inserite il cavo usb del vostro bay di recupero con il disco in formato ext3. :-))

A questo punto, vi bastera' aprire Esplora Risorse e selezionare la lettera di drive assegnata

temporaneamente al bay disco connesso tramite porta usb.
La visualizzazione e' praticamente identica a quella usata sui filesystem Windows, quindi anche la copia e il trasferimento dei files e' praticamente identico. :-)

Questo driver, puo' venire utilizzato nel computer forensic per leggere partizioni ext3 di linux sui sistemi windows, che altrimenti, segnalerebbero che il disco e' vuoto e proporrebbero all'utente di formattarlo con filesystem NTFS per poterlo leggere... :-))

Usando invece questo driver per recuperare dati Linux, risulta molto utile anche nelle assistenze informatiche che io definisco "speciali", e quindi potete mettere un segno di spunta su questo driver che vi permettera' di scoprire i segreti contenuti nelle partizioni Linux... :-))

A questo punto, molti di voi si staranno chiedendo se Linux e' sicuro, a tutti coloro che se lo stanno chiedendo, rispondo che anche Linux ha i suoi problemi di sicurezza, ma e' comunque molto piu' "sicuro" in rapporto ai sistemi Windows. :-)
Tutti i sistemi sono ritenuti "sicuri", l'importante e' che non trovino un tapiro di rete come me' che puo' dimostrare il contrario... ;-)))

Cari bloggers, anche per oggi e' tutto, buona navigazione a tutti voi, e cercate di non sbirciare troppo i dati riservati degli altri... ;-))

Sistemi operativi: Backup e ripristino dati con REDO Backup&Restore.

Post n°37 pubblicato il **18 Giugno 2012** da exodus1984
Carissimi bloggers, oggi parliamo di RedoBackup, un piccolo gioiello da tenere sempre a portata di mano nella cassetta degli attrezzi informatici per le nostre assistenze.

Come al solito andiamo a visitare la pagina del produttore per il download:

http://redobackup.org/download.php

la versione attuale e' la: redobackup-livecd-1.0.3.iso

RedoBackup, si differenzia da Clonezilla solo per l'interfaccia, mantenendo il motore di backup portato da questo sistema, l'interfaccia su Clonezilla e' testuale, mentre su RedoBackup e' grafica, ma fanno sempre lo stesso lavoro...:-))

Quindi, visitate il sito e scaricate subito questa immagine .iso, se avete vecchi computer e volete trasferire i dati, questo e' un ottimo sistema per farlo.

Per masterizzare l'iso da Windows, potete usare il mitico programma InfraRecorder, scaricabile da qui:

http://infrarecorder.org/

InfraRecorder e' un software open source disponibile in 35 lingue, dotato di una semplice interfaccia grafica essenziale e disponibile per tutti i sistemi operativi moderni.

Cari bloggers, anche per oggi ho postato un semplice articolo, e visto che il mio tempo e' poco, non ho potuto approfondire questo sistema come avrei voluto, ma i prossimi articoli saranno certamente piu' interessanti e completi.
A tutti voi un saluto e come sempre una buona navigazione. :-))

Sistemi operativi: proteggiamo i nostri dati da occhi indiscreti con TrueCrypt.

Post n°36 pubblicato il **18 Giugno 2012** da exodus1984
Carissimi bloggers, oggi tratteremo uno dei programmi di cifratura dati a livello personale piu' usato su ogni sistema operativo moderno, ma se cercate bene su internet, ne' trovate molti altri... :-)

Questo programma, permette di creare dischi cifrati con al loro interno altri dischi cifrati nascosti, si possono anche creare CDrom e DVD criptati, in modo da mantenere al sicuro il contenuto di questi media e poterli trasportare in sicurezza.

Il suddetto programma e' il famoso TrueCrypt, che possiamo prelevare da questo sito web:

http://www.truecrypt.org/downloads

Sulla pagina di download, dovrete scegliere il vostro sistema operativo usato e quindi procedere al download del programma dedicato alla vostra specifica macchina.

Con TrueCrypt, vengono usati sistemi a cifratura simmetrica, ovvero la stessa chiave per cifrare e la stessa per decifrare al volo tutti gli archivi criptati, pur mantenendo tali archivi completamente cifrati per ovvi motivi di sicurezza... :-)

Questo, porta a produrre archivi criptati che posti su un CD/DVD, possono essere solo decriptati da chi possiede la password, mentre il sistema operativo, non riconosce il supporto caricato sul lettore CD... :-))

Le chiavi usate con TrueCrypt, possono essere di diverso tipo, ma i due tipi usati, svolgono molto bene il loro lavoro:

1) password unica del tipo:
"IlmioGattomiHaGRAFFiatonellontano07/06/1984"

2) Keyfile monolitico:
creazione di una password impossibile da gestire a mano e creata
appositamente generando rumore informatico e codice binario casuale
e quindi salvata su chiave usb da 4 giga(grandezza minima della password)

A questo punto, introduciamo una breve parentesi di quello che rappresentano i programmi di cifratura nel mondo di internet:

Pagamenti con carte di credito, protocolli sicuri(SSL), canali cifrati, sono tutte implementazioni gestite dalla cosiddetta criptologia moderna.
La criptologia, si puo' definire la scienza che studia la crittografia e la crittoanalisi.

La crittografia, e' il modo in cui si comunica o si puo' comunicare segretamente utilizzando un insieme di cifrari predefiniti tra le parti in gioco, mentre la crittoanalisi e' il modo in cui si possono decifrare queste comunicazioni segrete.

La criptologia quindi, fa' parte del nostro vivere quotidiano su internet, anche se molte persone non lo sanno o semplicemente non sono informate.
Ci sono pero' dei compromessi al riguardo tra un utilizzo di cifrari matematicamente sicuri e le applicazioni che gestiscono la nostra vita su internet.

Per cui, se volete mantenere la vostra liberta' di espressione, cominciate ad usare questi programmi, usate sempre canali criptati, e rendete la vita difficile a chi vuole controllare i vostri pensieri e le vostre azioni, di qualunque ente si tratti(governativo o altro), la vostra vita appartiene solo a voi. :-)

Leggete queste poche righe per capire il motivo per cui sono necessarie reti cifrate e libere al di fuori del controllo di tutti, fonte:
http://it.wikipedia.org/wiki/Pagina_principale:

####

PARERE DELLA IX COMMISSIONE PERMANENTE
(Trasporti, poste e telecomunicazioni)

La IX Commissione,

esaminato, per le parti di propria competenza, il nuovo testo del disegno di legge recante: «Norme in materia di intercettazioni telefoniche, telematiche e ambientali» (n. 1415-B Governo),

premesso che:

il testo approvato dal Senato reca modifiche al comma 29 dell'articolo 1, in base alle quali si precisa che i giornali quotidiani e periodici diffusi per via telematica sono compresi nell'ambito dei siti informatici ai quali è esteso l'obbligo di rettifica delle informazioni ritenute non veritiere o lesive della reputazione dei soggetti coinvolti, mediante la pubblicazione, entro quarantotto ore dalla richiesta, delle dichiarazioni o rettifiche con le stesse caratteristiche grafiche, la stessa metodologia di accesso al sito e la stessa visibilità della notizia cui si riferiscono;

la formulazione del testo, come modificato dal Senato, non esclude il rischio, già evidenziato nel parere espresso dalla Commissione sul disegno di legge in prima lettura presso la Camera dei deputati, che l'obbligo di rettifica ricada, per la generalità dei siti informatici, piuttosto che sugli autori dei contenuti diffamatori, sui gestori di piattaforme che ospitano contenuti realizzati da terzi, i quali, in considerazione del volume dei contenuti ospitati dalla piattaforma, non sarebbero in grado di far fronte a tale obbligo;

Con questo, chiunque crei un sito web o un blog considerato lesivo nei confronti magari del governo, sarebbe costretto ad alterarlo, anche se il contenuto, non e' il suo pensiero da cui il blog o il sito e' scaturito... :-(

I provider, dovrebbero adeguarsi, limitando la liberta' espressiva dei loro
utenti, con conseguenze disastrose per i bloggers ritenuti "offensivi" o per i siti web ospitati su un server in cui vi sono pubblicate immagini non ritenute adeguate da qualcuno... :-(

Ci sono reti cifrate utilizzabili in ogni parte del mondo, e la censura di rete e' sempre in agguato, ma la

censura e' controllo, e quindi moltissimi siti web vengono costruiti su reti cifrate, mandando i link sulla rete internet normale e indicando i modi e i tipi di cifratura utilizzata per poterli connettere. :-)

Cari bloggers, anche per oggi e' tutto, e che la liberta' informatica possa essere la vostra luce nel nuovo mondo di internet. :-)

Archivi compressi e problemi di decompressione: risolviamoli con Universal Extractor.

Post n°38 pubblicato il **20 Giugno 2012** da exodus1984
Carissimi bloggers, anche oggi continueremo con la selezione di applicazioni molto utili per il nostro sistema Windows.

Oggi parleremo di un programma che ci sara' molto utile quando avremo a che fare con formati file compressi e zippati... ;-))
Molte volte, ci troviamo di fronte a degli ostacoli che non riusciamo a superare proprio perche' i formati dei files sono compressi e non disponiamo del programma decompressore per estrarre il loro contenuto, oppure semplicemente il programma per aprirli e' troppo costoso per le vostre tasche... :-))

Come di consueto, andiamo a visitare il sito web per il download:

http://legroom.net/software/uniextract

La versione corrente e' la 1.6.1, potete scaricare anche il codice sorgente, l'archivio binario che viene utilizzato per le assistenze informatiche su key usb portatile ed infine, l'installer setup per i sistemi windows statici.

Questo programma e' stato creato per rimediare agli inconvenienti della linea di comando e rendere facile l'estrazione di archivi compressi a tutti gli utenti non tecnici, allo stesso tempo, sono stati riuniti moltissimi formati compressi che si possono aprire con un unico tool invece di avere decine di programmi di compressione/decompressione su cui bisognava ricordarsi tutti gli switch per effettuare una semplice operazione di estrazione dati.

Per l'installazione della lingua d'origine, dovrete scaricare il file "Italian" e copiarlo nella directory di localizzazione descritta nella pagina di Uniextract.

Questo programma usa un identificatore di files chiamato TrID, la pagina di documentazione e' questa:

http://mark0.net/soft-trid-e.html

Tornando al programma trattato oggi, il sistema puo' leggere diverse estensioni di files, ecco un breve elenco, cosi' potete capire se questo programma potrebbe esservi utile:

Archive Type Common File Extension(s)
7-zip archive .7z, .exe
ACE archive .ace, .exe
ARC archive .arc
ARJ archive .arj, .exe
ASpack compressed file .exe
BIN/CUE CD-ROM image .bin, .cue
bzip2 archive .bz2, .tbz2, .tar.bz2
CPIO compressed file .cpio
Debian package .deb
DiscJuggler CD-ROM image .cdi
Encoded files .b64, .uu, .uue, .xx,
.xxe, .yenc, .ntx
Gentee package .exe
gzip archive .gz, .tgz, .tar.gz
IMG floppy disk image .img
Inno Setup package .exe
Installer VISE package .exe
InstallShield Cabinet archive .cab, .1, .lib
InstallShield package .exe
ISO 9660 CD-ROM image .iso
KGB archive .kgb, kge, .exe
LZH compressed file .lzh, .lha
LZMA compressed file .lzma
LZO compressed file .lzo

LZW compressed file .Z, .tz, .tar.Z
LZX compressed file .lzx
MHTML file .mht
Microsoft Cabinet archive .cab, .exe, .imf
Microsoft Compiled Help file .chm
Microsoft compressed file .??_
Microsoft LIT e-book .lit
Microsoft Windows Help file .hlp
HTC NBH ROM image .nbh
Nero CD-ROM images .nrg
NSIS package .exe
Oasis Document Format (ODF) document .odt, .odp, .odg, .ods
Office Open XML (OOXML) document .docx, .pptx, .xlsx
Outlook Express mail archive .dbx
PEA archive .pea
RAR archive .rar, .001, .exe
Reflexive Arcade package .exe
RoboForm package .exe
RPM package .rpm
SetupFactory package .exe
SIS (SymbianOS) packages .sis
StuffIt packages .sit
TAR archive .tar, .tbz2, .tgz, .txz, .tz,
.tar.bz2, .tar.gz, .tar.xz, .tar.Z
UHARC archive .uha
UPX compressed file .exe, .dll
Windows Imaging Format image .wim
Windows Installer merge module .msm
Windows Installer package .msi
Windows Installer patch .msp
Windows Update Standalone patch .msu
Wise Installer package .exe
XZ compressed file .xz, .txz, .tar.xz
ZIP archive .zip, .jar, .xpi, .wz, .exe
Zoo archive .zoo

Se avete trovato l'estensione che vi serve, allora prelevate il programma e iniziate a decomprimere i vostri archivi. :-)

Cari bloggers, anche per oggi e' tutto, a tutti voi, una buona permanenza su internet. :-)

Computer e emulazione facciale: come fare uno scherzo tecnologico agli amici :-)

Post n°39 pubblicato il **21 Giugno 2012** da exodus1984
Carissimi bloggers, oggi parleremo di un software che ci permette di usare il computer e leggere i nostri libri elettronici semplicemente usando il riconoscimento facciale e la gestualita' del volto per aprire, leggere, chiudere documenti rimanendo con le mani completamente libere. :-)

Questo vuol dire niente piu' uso del mouse, perche' potreste procurarvi la famigerata "artrite da topo" per i troppi click... ;-))
A parte gli scherzi, questo software, mi e' servito la scorsa settimana per fare uno scherzo ad un amico non troppo portato con questo genere di tecnologia. :-)

Le cose sono andate all'incirca in questo modo, visto che dovevo fare un'assistenza informatica al computer dell'amico, ho buttato l'esca dicendogli:

io: "ma tu usi ancora il mouse?"
lui: "scherzi? e cos' altro dovrei usare secondo te???"
io: "il tuo pc e' vecchio, oggi i computer si gestiscono con la forza del pensiero..." ;-))
lui: "tu mi vuoi prendere in giro..."
io: "niente affatto, guarda qui..." 8-))

Il programma di cui parleremo oggi ha fatto questo effetto su molte persone che lo hanno visto in azione, anche perche' ho dovuto compilare una mia versione personale per portarlo sul mio hardware modificato a 64 bit.

L'amico, non credeva a quello che stava vedendo con i suoi occhi, mentre io che sono un grosso burlone, continuavo lo scherzo senza nessuna pieta'... :-))

"Mi devo concentrare sulla directory degli e-book", "Ecco, ora sto' pensando di aprire il libro di analisi matematica", detto e fatto, l'amico, sempre piu' curioso e sgomento, : "ma cosa... ma come... non e' possibile...", e io:"devo solo concentrare il mio pensiero per guidare il puntatore..."(8-))

La notizia che che io usavo il computer con "la forza del pensiero", ha fatto il giro dell'isolato, e quindi mi sono ritrovato a chiarire tutta la situazione spiegando questa tecnologia e il suo funzionamento a tutti dopo avere offerto loro da bere...(chi la fa', l'aspetti...) ;-)))

Tornando al nostro programma, potete trovarlo a questo indirizzo web:

http://eviacam.sourceforge.net/eviacam.php

Le piattaforme attualmente supportate sono queste:

GNU/Linux
Windows 2000/XP/Vista/7

I files in archivio sono questi:

http://sourceforge.net/projects/eviacam/files/eviacam/1.5.4/

README
eViacam-1.5.4.exe
eviacam_1.5.4-1_source.changes
eviacam_1.5.4-1_i386_debian_squeeze.deb
eviacam_1.5.4-1.debian.tar.gz
eviacam_1.5.4-1.dsc
eviacam_1.5.4.orig.tar.gz

Come ho detto in precedenza, ho dovuto compilare una versione particolare per il mio hardware, in quanto, sul sito di download mi dava solo la possibilita' di avere l'installer per l'architettura I386, mentre per quella a 64 bit, dovrete scaricarvi i sorgenti, caricare le relative librerie, e compilarvi il loader

principale e il programma di gestione e configurazione.

Questo programma, usa il riconoscimento facciale, e dopo la prima configurazione del volto dell'utente, si passa alla modalita' in cui si puo' avere il click per aprire(1/2click), per scorrere i documenti, per spostare le icone del desktop solamente indicando e guardando la posizione dove metterle. :-)

La precisione di puntamento, dipende in gran parte dalla telecamera, se avete un webcam HD e un framerate di almeno 25 fps, il risultato e' sorprendente, altrimenti, io che ho testato vecchie webcam a bassa risoluzione, il funzionamento e' quasi uguale, ma il sistema e' piuttosto lento, e tende ad avere una risposta non adeguata.

La distanza dallo schermo, puo' essere di circa 40/50 cm, ma a quasi 1 metro dallo schermo, il risultato cambia, perche' i tremori naturali del volto umano, interagiscono con il software, sbagliando il puntamento.

Le condizioni di illuminazione statica della telecamera, sono molto importanti perche' permettono di localizzare un volto anche a circa 2 metri dallo schermo(23 pollici), ma se oscurate la vostra telecamera con un dito sull'obiettivo, il programma non vede piu' nulla e potete ritornare al vostro amato mouse senza problemi. :-))

Il riconoscimento facciale, puo' essere configurato sia in modo automatico che in modo manuale, scegliete il modo manuale per aggiustare tutti i parametri che ritenete opportuni, dal modo di fare click, al modo di osservare una parte dello schermo che vi interessa.

Cari bloggers, anche per oggi e' tutto, buon divertimento a tutti voi e come sempre, buona navigazione su internet. :-))

P.S. ...E non fate scherzi del ca...volo agli amici... 8-))

Racconti Hacker: la fantascienza nel mondo pirata.

Post n°40 pubblicato il **23 Giugno 2012** da exodus1984

Carissimi bloggers, il mio pallino per i racconti dedicati alla rete e agli hacker e' un punto fisso, per cui questa sera vi mando un racconto di fantascienza hacker. :-)

Questi racconti, vengono condivisi con licenza CCPL, e sono raccolti in formato cartaceo per la formazione di piccoli volumi che creo a livello personale.

Buona lettura a tutti. :-)

HERCULES

La nave esplorativa Comae Berenicis scivolava nel silenzio del cosmo, l'impero terrestre si trovava di fronte ad una guerra galattica per la quale nessun essere umano o unita' sintetica geneticamente modificata, avrebbe potuto avere scampo.

Erano tempi molto duri, il traffico di schiavi Zakrin, aveva aperto una breccia nei confini dell'impero terrestre, portando i nemici Argast nel cuore stesso dell'impero, facendolo cadere un pezzo alla volta.

La minaccia continua e le continue imboscate alle navi da trasporto imperiali, avevano creato uno stato di fragilita' nella popolazione umana distribuita in tutta la galassia.

Il comandante Xylbe ordino' di controllare i supporti vitali e i sistemi di difesa.

Il trasporto a lei affidato, era di vitale importanza per la sopravvivenza dell'impero, ma avrebbe anche messo fine alla guerra stessa.

Yanix Xylbe, 18 anni, il piu' giovane comandante donna della flotta imperiale terrestre, aveva sulle spalle il destino dell'intero universo conosciuto.

Era entrata in accademia a 15 anni, nei due anni successivi, aveva preso il brevetto di volo intergalattico e partecipato a numerosi combattimenti contro gli incursori Argast in molti sistemi stellari appartenenti all'impero terrestre.

Prima del compimento del suo diciottesimo compleanno, la sua unita' da combattimento era stata gravemente colpita, e Yanix aveva riportato mutilazioni in molte parti del corpo.

Fu' cosi' che venne prima ricostruita e poi riassegnata alle unita' da trasporto intergalattiche.

Le strumentazioni automatiche della nave si stavano preparando ad eseguire un salto a curvatura spazio-temporale, la nave doveva consegnare il suo prezioso carico prima dell'arrivo degli Argast.

Erano solo in due i passeggeri, il comandante Xylbe e il carico che trasportava.

Yanix controllo' ancora una volta il suo prezioso passeggero, un Hacker mutante che aveva violato i sistemi di comunicazione degli Argast, ritenuti inviolabili dai piu' grandi scienziati dell'impero terrestre.

Klab Rekh, un Hacker mutante, originario di uno sperduto pianeta ai confini dell'impero terrestre, era l'ultima carta che la Terra poteva giocarsi in questa guerra galattica che durava ormai da piu' di 300 anni.

I miliardi di vite perse tra le due fazioni in guerra, non avevano portato a nessuna tregua, tutti i tentativi per ristabilire la pace nell'universo erano miseramente falliti.

La nave era diretta nella costellazione di Ercole, per fermare in modo definitivo gli aggressori Argast.

Yanix ordino' il salto a curvatura, e mentre la nave diventava energia, un pensiero volo' dritto alla mente telepatica di Klab.

Un anno prima, mentre Yanix combatteva gli Argast ai confini dell'impero, fu' abbattuta su Krah, il pianeta natale di Klab, fu' proprio klab a trovarla e a salvarle la vita, furono convocati i migliori dottori Hacker del pianeta, che con le loro modifiche e le loro creazioni, permisero a Yanix di sopravvivere e di poter tornare in servizio.

Lei, un'umana cyborg, lui, un hacker mutante, si erano giurati eterno amore in una semplice cerimonia prima della partenza dal pianeta della Comae Berenicis.

Per salvare l'impero e riportare la pace nella galassia, esisteva un solo modo, distruggere la stella sacra agli Argast da cui traevano la loro energia.

Solo allora si sarebbero arresi, e l'universo avrebbe ritrovato la pace.

Questa missione, era stata assegnata loro dal consiglio di guerra dell'impero, Klab doveva distruggere la fonte di energia degli Argast mentre Yanix avrebbe dovuto proteggere in questo ultimo e disperato tentativo le colonie esterne dalle incursioni degli Argast.

A 240 anni luce dalla Terra, l'energia della nave ritorno' materia, la Comae Berenicis aveva mutato la sua configurazione da trasporto a nave da guerra e sotto la luce di una gigante rossa si sarebbe deciso il destino di milioni di civilta' aliene diverse.

Klab attivo' la rete molecolare, puntando il bersaglio.

Alfa Herculis, una supergigante rossa, con un diametro di 600 volte il nostro Sole, stava per essere distrutta dagli impulsi contrapposti nucleari provenienti dai macchinari di Klab.

Gli Argast risposero al fuoco di copertura su Klab, la Comae Berenicis si trasformo' in una palla di fuoco nucleare, mentre Yanix raggiungeva Klab con il modulo di salvataggio.

Un pensiero raggiunse la mente di Yanix: "Sono troppo lontano, non riesco ad innescare il processo di implosione della stella...".

"Klab, dobbiamo portarci nel campo gravitazionale interno della stella..."

Con le lacrime agli occhi, Yanix aggancio' il modulo di Klab, e mentre una delle navi Argast faceva fuoco, un lampo di luce si levo' da Alfa Herculis cancellando per sempre la piu' grande minaccia mai esistita per l'impero terrestre.

La guerra era finalmente finita, e la pace sarebbe tornata a regnare per sempre, per merito dell'amore di due ragazzi che donarono le loro vite per la salvezza dell'universo.

Cari bloggers, spero che il racconto sia stato di vostro gradimento e come sempre, buon divertimento a tutti. :-)

Riflessioni personali: analisi di una stella chiamata Sole.

Post n°41 pubblicato il **01 Luglio 2012** da exodus1984
Carissimi bloggers, oggi vorrei fare una riflessione in merito ad alcuni passaggi obbligati della nostra stella principale, il Sole.

Il nostro Sole, che molto probabilmente faceva parte di un ammasso globulare aperto, e' nato circa 4600 milioni di anni fa'.
La nostra stella, nata da una nebulosa contenente idrogeno ed elio nelle giuste proporzioni, ricava la sua energia da reazioni nucleari che trasformano l'idrogeno in elio, una versione "aperta"(Open Source) rispetto alle reazioni che avvengono in una normale bomba all'idrogeno, che sono molto simili in questo caso.

Per creare una stella, le condizioni della materia, devono seguire una costante universale, un semplice ammasso di gas idrogeno/elio che abbia una massa di circa il 6 percento di quella del nostro Sole, non potra' innescare il processo nucleare, proprio perche' la condizioni al suo interno, non sono sufficienti perche' questo possa avvenire.

La costante universale del 6 percento, delimita la classificazione tra i pianeti e le stelle, questo ci porta ad una conclusione logica, se Giove che ha la stessa composizione chimica del Sole, avesse avuto una massa di circa 60 volte superiore a quella che ha, sarebbe potuto diventare la seconda stella del nostro sistema solare.

Questo fatto, potrebbe sconvolgere l'equilibrio gravitazionale che il nostro Sole esercita sui corpi del sistema solare, la gravita' contrapposta di due stelle distanti solo poche unita' astronomiche tra di loro, avrebbe certamente creato dei problemi seri allo sviluppo della vita sulla Terra.

La massa di una stella e' un fattore di vitale importanza, perche' influisce direttamente sulla temperatura, sulla luminosita' e sulla durata di vita della stella stessa.
Per cui, una stella con una massa di un decimo quella del nostro Sole, viene definita "nana rossa", e ha una temperatura superficiale di circa 3000-3500 gradi C°.

Le stelle che hanno una massa minore di quella del Sole, sono anche quelle che vivono di piu', circa un milione di milioni di anni, quasi 100 volte la vita stimata del nostro Sole.
La temperatura del nostro sole e' di circa 5500 gradi in superficie, mentre le reazioni nucleari al suo interno sono stimate sui 15 milioni di gradi, la vita prevista della nostra stella, e' di 10.000 milioni di anni, allo stato attuale, siamo a quasi meta' della sua vita, e tra 5 miliardi di anni il suo ciclo vitale arrivera' alla fine.

Il Sole a questo punto, si espandera' nel sistema solare distruggendo tutto quello che trovera', alla ricerca di combustibile le sue reazioni nucleari si disperderanno nel cosmo, formando un anello di fumo detto "nebulosa planetaria", anche se cio', non ha nulla a che vedere con i pianeti.
Il Sole, diventato ormai una gigante rossa, ovvero una stella che sta' per morire, potrebbe trasformarsi anche in altri oggetti differenti.

Il nostro Sole, e' quindi destinato a diventare una "nebulosa planetaria" prima di diventare una nana bianca?
Potrebbe essere, ma le stelle che hanno raggiunto diverse masse solari(supergiganti) sono soggette ad una fine molto spettacolare, quando diventano delle splendenti supergiganti, non hanno alcuna possibilita' di raggiungere lo stadio di nebulose planetarie, e la loro massa interna e' molto grande che le reazioni nucleari continuano in modo incontrollato finche' la stella diventa instabile ed esplode, questa esplosione stellare, viene chiamata "Supernova".

Tutto questo, ci porta a riflettere su molti aspetti della nostra esistenza, primo fra tutti, l'interrogativo di sempre:

Cosa succederebbe se il nostro Sole si oscurasse per sempre?

La vita sulla Terra finirebbe in meno di una settimana, perche' i processi nucleari del Sole, generano la vita ma la possono anche distruggere.
Questo, lasciando perdere che una reazione nucleare, porterebbe la massa del Sole direttamente sulla

Terra in circa 8,3 minuti, e quindi la previsione di vita sulla Terra di una settimana, e' molto ottimistica... ;-))

A questo punto, un pensiero giunge spontaneo, gli uomini combattono guerre, si distruggono tra di loro, e si credono al di sopra di tutto e di tutti, ma in realta' un evento cosmico di questo tipo e' sempre possibile, e nessuno puo' sfuggire a tutto questo, tutti noi, non siamo nemmeno "polvere di stelle", ma siamo parte di un ciclo infinito di vita e di morte dell'intero universo.

Cari bloggers, con questo vi lascio ai vostri pensieri e come sempre, buona navigazione a tutti voi.

Utility per i nostri Ebook: classifichiamo e scriviamo i nostri Ebook Con Calibre e Sigil

Post n°42 pubblicato il **02 Luglio 2012** da exodus1984

Carissimi bloggers, oggi parleremo di un programma in grado di leggere i nostri E-book preferiti, ma anche di creare formati e-pub da documenti personali come file .pdf e altro.

Questo programma ci permette per esempio di portare i libri che noi scriviamo sui nostri lettori di e-book portatili, in modo da poterli leggere e rivedere quando vogliamo.

La nuova versione di Calibre, puo' gestire un server di e-book, in modo che in qualunque parte del mondo ci troveremo, potremo sempre accedere alla nostra raccolta personale di libri elettronici.

Andiamo subito a visitare il sito web di Calibre:

http://calibre-ebook.com/download

Qui, potete scaricarvi le versioni che preferite per i sistemi operativi su cui lavorate, a vostra scelta.

La descrizione semplice di Calibre e' questa:

"calibre is a free and open source e-book library management application developed by users of e-books for users of e-books". :-))

Ma sotto l'aspetto semplice di Calibre, si nascondono vere e proprie funzionalita' da "programma definitivo"... ;-))

Tutto quello che dovete fare e' scaricarvi una versione per il vostro sistema operativo e cominciare ad esplorarla per vedere tutto cio' che e' possibile fare.

Calibre non e' un tool per la modifica e l'editing di quello che volete scrivere, e per questo, potete vedere altri tool come Sigil (pagina principale),che viene descritto cosi':

"Sigil is a multi-platform EPUB ebook editor with the following features"

Code license

GNU GPL v3

Content license

Creative Commons 3.0 BY-SA

http://code.google.com/p/sigil/

e quindi andate a vedere la versione di Sigil che volete scaricare:

http://code.google.com/p/sigil/downloads/list

Sigil-0.5.3-Mac-Package.dmg Mac Build 0.5.3 Featured Feb 25 Feb 25 47.7 MB 24080

Sigil-0.5.3-Windows-x64-Setup.exe Windows (x64) build 0.5.3 Featured Feb 25 Feb 25 12.8 MB 39450

Sigil-0.5.3-Windows-Setup.exe Windows build 0.5.3 Featured Feb 25 Feb 25 11.3 MB 64642

Sigil-0.5.3-Code.zip Source code package for 0.5.3 Featured Feb 25 Feb 25 12.2 MB 5752

A livello personale, ho portato diversi testi scritti anni addietro in formato e-pub, prima per fare delle prove e poi, dopo avere imparato bene questo programma, ho potuto creare direttamente i miei e-book per specifici dispositivi portatili che a seconda del tipo di hardware, possono o non possono mantenere tutte le caratteristiche costruttive del libro che vogliamo portare sul nostro dispositivo portatile.

Detto questo, Calibre non e' solo un lettore di e-book, ma mantiene la vostra collezione di testi elettronici e raccoglie notizie da internet in modo che se siete degli scrittori di racconti come il sottoscritto, potete prendere i vostri spunti creativi dalle notizie stesse di internet per creare una storia su cui basare il vostro prossimo libro... :-))

Usando Calibre, potrete inoltre convertire i vostri libri elettronici da un formato ad un altro senza troppi problemi, potrete cambiare le copertine, oppure convertire un'intera biblioteca di libri in un colpo solo.

L'ultima versione stabile di Calibre e' la 0.8.58 [29 Jun, 2012]

L'unico consiglio che vi posso dare riguardo a questo programma, e' quello di usarlo, usatelo per contribuire a migliorarlo e per avere sempre un programma di lettura rapido ed efficiente su tutti i sistemi operativi.

Cari bloggers, per oggi e' tutto, buona navigazione a tutti voi e buon divertimento su internet. :-)

Utility e manutenzione di sistema: ClamWin nelle assistenze informatiche di base.

Post n°43 pubblicato il **03 Luglio 2012** da exodus1984
Carissimi bloggers, oggi parliamo di un antivirus libero, creato per sistemi win32 e per le scansioni portatili dei sistemi windows.

Come sempre, andiamo subito sul sito di download:

http://sourceforge.net/projects/clamwin/files/clamwin/0.97.4/

Per tutte le altre informazioni tecniche, potete leggere la pagina principale del sito web dedicato :

http://it.clamwin.com/content/view/18/46/

Clamwin puo' essere portato su key usb per assistenze informatiche veloci, ma potete anche vedere Clam Sentinel, che provvede ad offrire un motore scanner in tempo reale, non disponibile con il semplice Clamwin.

Potete scaricarlo a questo link:

http://sourceforge.net/projects/clamsentinel/files/clamsentinel/1.19/

L'interfaccia di ClamWin, e' molto semplice, questo e' stato fatto in modo da avere una visuale di tutti i dischi fissi collegati al sistema, e di pianificare l'operazione di scansione antivirus come meglio credete.

Sul setup principale, potete inserire una directory di quarantena dove potete catturare tutti i virus che volete, per poterli poi aprire e classificare.

Le richieste di codice virale da parte degli sviluppatori, e' necessaria per l'ampliamento e la localizzazione di nuovi tipi di virus informatici non ancora conosciuti.

Quindi, se siete cacciatori di virus informatici, questo piccolo programma portatile, vi sara' molto utile nelle vostre assistenze informatiche per catturare, archiviare e analizzare il comportamento virale di un agente patogeno informatico. :-)

Infine, l'aggiornamento del database virale e' sempre disponibile su internet, e per la versione portatile, basta solo far partire ClamWin dalla chiavetta USB e far eseguire l'aggiornamento con una connessione internet attiva.

L'uso che ne' ho fatto di questo programma e' davvero molto speciale, infatti ho catturato virus informatici per poterli studiare, dando un valido contributo allo sviluppo di questo stupendo programma.

Potete aiutare lo sviluppo in molti modi diversi, dovete solo leggere sulla pagina principale il modo che piu' va' bene a voi e al vostro modo di lavorare.

Anche per oggi e' tutto, cari bloggers, di nuovo, buona navigazione e buon divertimento a tutti voi. :-)

Progettazione del nostro spazio abitativo: come creare la nostra casa e le nostre stanze con SweetHome3D.

Post n°44 pubblicato il **06 Luglio 2012** da exodus1984

Carissimi bloggers, anche oggi faremo una breve recensione di un programma che mi e' stato molto utile per ri-configurare le stanze della casa ed avere un'anteprima di come sarebbe stato il risultato finale.

Oggi, parleremo di SweetHome3D, un ottimo programma per la progettazione e la ristrutturazione di ambienti vecchi e nuovi.

Disponendo delle misure delle vostre stanze, potete ricrearle virtualmente e apportare tutte le modifiche che vi servono per ottenere la casa, la stanza, e i locali che desiderate creare.

L'interfaccia utente di SweetHome3D, rappresenta quanto di meglio potremo aspettarci da un programma di questo tipo, ovvero: semplicita' costruttiva, catalogo dell'arredamento interno molto ben fornito, piantina della casa da costruire, ed infine una vista 3D del progetto che avete appena creato.

I quattro pannelli principali visualizzati dal programma, possono essere usati in modo semplice e diretto, a seconda di quello che state facendo, o sulla piantina o se state scegliendo l'arredamento interno per il vostro progetto.

La grande semplicita' di questo programma, e' che puo' essere usato da tutti, non solo da utenti tecnici e geometri, una volta aperto il programma, avrete subito a disposizione tutto quello che vi serve per creare il vostro progetto, dalla semplice stanza dei bambini, alle stanze adibite a laboratorio(il mio caso...).

Quindi, se vi ricordate le lezioni di geometria imparate alle scuole elementari, sarete operativi in meno di 5 minuti, e poi, avrete solo il limite della vostra fantasia per creare, modificare e arredare tutti gli ambienti che volete progettare e costruire.

Per il catalogo degli oggetti, fate riferimento al sito web del programma, ci sono moltissime altre librerie che si possono importare per aggiungere non solo l'arredamento, ma anche cani,gatti, cavalli etc.etc... :-))

Per queste librerie esterne al programma, dovrete vedere con quale licenza vengono distribuite, visto che sono creazioni esterne di utenti/professionisti del settore immobiliare.

A questo punto, e' giusto indirizzare i bloggers sul sito di SweetHome3D:

http://www.sweethome3d.com/it/index.jsp

Ora, potete passare a scaricare il programma per provarlo, guardate il tipo di installer per il vostro sistema operativo e procedete:

http://www.sweethome3d.com/it/download.jsp

Se non avete installato i driver per la vostra scheda video, il programma funziona bene comunque, ma la vista 3D risulta non troppo fluida e la navigazione potrebbe essere "a scatti", in ogni caso, per chi come me' bada al sodo, ovvero se siete progettisti, vi basta solo la planimetria della stanza/casa per vedere se il vostro progetto e' come voi lo desiderate.

La vista 3D rimane in ogni caso un buon sistema se dovete creare piantine virtuali per far visitare un luogo ad utenti internet.

Potete poi condividere i progetti che avete creato con altri utenti, che da questi, possono partire e modificare altri aspetti del progetto (lavoro di gruppo).

Cari bloggers, anche per stasera e' tutto, buona navigazione a tutti voi e buon divertimento su internet. :-)

Riflessioni personali: trovare il mio tempo per fare le cose che vorrei... :-)

Post n°45 pubblicato il **07 Luglio 2012** da exodus1984

Carissimi bloggers, anche per oggi vi mando un piccolo pensiero personale:

AuFF... CHE CALDO!!!! :-)))

Vabbe', queste ultime settimane, sono state davvero faticose, il caldo, l'afa, la voglia di fare e il tempo che non ho mai a mia disposizione... ;-))

Oggi stavo tranquillamente smanettando un computer in santa pace, e all'improvviso, mi capita una visita del tutto inaspettata, un vecchio volpone che mi propone di scrivere un libro... :-)

Allora ci mettiamo a discutere le impostazioni, la trama e alla fine, ci si accorda per una ormai classica storia ai limiti della fantascienza(...e mi pareva strano....) :-)

Per cui io gli dico che se ci mette dentro qualche Hacker posso anche valutare la prima stesura della trama, ma lui non ci crede molto e quindi passiamo alle impostazioni tecniche finali: copertina principale e una prefazione in grado di catturare il lettore prima ancora che possa avere letto il primo capitolo del libro... :-)

Azz... io che volevo dedicare l'intero pomeriggio allo spippolamento del computer, non avevo in programma questa visita, e quindi sono rimasto un po' sviato dai miei intenti informatici, per cui, non ho potuto fare la festa a questo povero computer... :-(

Domani e' domenica, sveglia all'alba come progetto iniziale della giornata, modifica e smanettamento completo del computer, prima che venga a trovarmi qualche altro amico, e che mi proponga altre cose strane... :-))

Volete sapere come e' finita la visita di oggi?

Ho accettato di leggere alcuni capitoli iniziali per fare una verifica e di come poter presentare questo libro scrivendo una prefazione accattivante per i lettori. Credo che una storia basata sul mondo moderno reale di oggi, sia molto piu' attraente se ci mettiamo in mezzo anche qualche Hacker e la rete Internet... ;-))

Sarebbe certamente anche piu' credibile da parte dei lettori, visto che tutti quanti conoscono la rete e usano programmi informatici.

Con questo, cari bloggers, per oggi vi saluto tutti, visto che domani sara' una domenica di fuoco informatico... ;-))

Buona navigazione a tutti voi e come sempre, buon divertimento. :-)

Utility per Linux/windows: Impariamo ad utilizzare PeaZip nelle assistenze informatiche.

Post n°46 pubblicato il **08 Luglio 2012** da exodus1984

Carissimi bloggers, anche oggi facciamo una breve recensione software, questa volta tocca a PeaZip, un'utility che puo' fare molte cose con i nostri files, dalla semplice decompressione/compressione dati di oltre 150 formati diversi al backup dati, per finire con la crittografia forte dei nostri dati piu' sensibili.

Ma le opzioni di PeaZip, non sono finite qui, potete avere il programma in codice sorgente e ri-compilarlo per architetture diverse se non potete portare direttamente gli archivi binari gia' pronti per i piu' comuni sistemi operativi.

Per le assistenze informatiche su sistemi GNU/Linux, ho scelto di caricare la versione portatile di PeaZip che dispone di una semplice interfaccia grafica a seconda dell'ambiente X che potete trovare sulle varie distribuzioni Linux.

Oggi, analizzeremo questa versione portatile, che e' quella che uso di piu' e quindi anche quella che conosco meglio.

Di solito lavoro su ambienti GTK2, ma trovate gli archivi anche per le interfaccie grafiche basate su QT4.

Dovete solo vedere l'ambiente grafico che il sistema del cliente porta sul suo Desktop e quindi, agire di conseguenza scaricando la versione che vi serve per quella particolare assistenza informatica.

Andiamo quindi come sempre a visitare la pagina principale del sito web ufficiale di PeaZip:

http://www.peazip.org

la pagina per il supporto/help:

http://www.peazip.org/peazip-help.html

E quindi andiamo a vedere l'archivio che ci serve, scaricandolo da questo link:

sourceforge.net/projects/peazip/files/4.6/

peazip-4.6.WINDOWS.exe	2012-06-13	9.1 MB
peazip-4.6.WIN64.exe	2012-06-13	9.3 MB
peazip_portable-4.6.WINDOWS.zip	2012-06-13	7.1 MB
peazip_portable-4.6.WIN64.zip	2012-06-13	7.2 MB
peazip-plain-4.6.WINDOWS.exe	2012-06-13	4.7 MB
peazip-plain-4.6.WIN64.exe	2012-06-13	4.8 MB
peazip_help.pdf	2012-06-13	1.2 MB
peazip-4.6.src.zip	2012-06-13	2.6 MB
peazip-4.6.about_translations.zip	2012-06-13	577.5 kB
peazip-4.6.spec	2012-06-13	2.7 kB
peazip_portable-4.6.LINUX.GTK2.tar.gz	2012-06-13	9.5 MB
peazip_4.6.LINUX.GTK2-2_all.deb	2012-06-13	9.9 MB
peazip_4.6.LINUX.GTK2-2_i386.deb	2012-06-13	9.9 MB
peazip-4.6.LINUX.GTK2-1.i386.rpm	2012-06-13	9.9 MB
peazip-4.6.LINUX.GTK2.tgz	2012-06-13	10.0 MB
peazip_portable-4.6.LINUX.Qt.tar.gz	2012-06-13	8.6 MB
peazip_4.6.LINUX.Qt-2_i386.deb	2012-06-13	9.5 MB
peazip-4.6.LINUX.Qt-1.i386.rpm	2012-06-13	9.5 MB
peazip-4.6.LINUX.Qt.tgz	2012-06-13	9.6 MB

Visto che trattiamo la versione portatile, ma considerando che compilando i sorgenti, possiamo avere anche un'installazione di livello fisso sul nostro computer, l'unica differenza e' che gli archivi binari portatili sono da preferire alla compilazione statica, in quanto, ci servono proprio per fare determinate operazioni sui PC, senza installare nulla in piu' sul sistema del cliente.

A livello nativo, PeaZip e' in ogni caso gia' stato costruito come "applicazione portatile", quindi, se non volete caricarvi troppo con una compilazione del codice sorgente, i binari statici del programma, vanno benissimo. :-)

Se invece siete degli inguaribili smanettoni romantici e pirati, allora dovete sapere che Peazip e' stato sviluppato in codice Free Pascal, usando un ambiente RAD come Lazarus, per cui, se decidete di seguire questa strada, allora dovete dare un'occhiata a questi link:

http://www.peazip.org

http://code.google.com/p/peazip/

PeaZip si puo' integrare molto bene sia con ambienti Desktop come Gnome che con KDE, per cui, sono coperte tutte le distribuzioni GNU/Linux principali.

Ho usato un archivio peazip_portable-4.6.LINUX.GTK2.tar.gz, ma come ho detto in precedenza, questo dipende da quale interfaccia grafica gira sul computer sotto esame.

Possiamo cambiare la localizzazione andando sotto Options->Localization e quindi cliccare su it.txt per avere la traduzione in lingua italiana.

Per le password di cifratura, si possono creare keyfiles fino a 4096 bit e trasportarli su chiavi usb per essere usati solo quando servono a voi per aprire/chiudere un documento riservato.

Anche per oggi e' tutto cari bloggers, di nuovo, buona domenica a tutti e buona permanenza su internet. :-)

Post di pre-riscaldamento ;-))

Post n°48 pubblicato il **31 Agosto 2012** da exodus1984
Carissimi bloggers, un breve post di pre-riscaldamento per prepararci ad una nuova ed entusiasmante stagione informatica invernale(quasi) sui blog di Libero. :-)

Presto potro' riprendere con gli articoli di natura informatica, ma prima vorrei regalarvi qualcosa di utile.

Le sorprese come sempre, le potrete trovare nei prossimi post. :-)

A tutti voi, un buon proseguimento e una buona navigazione su internet.

Backup e Restore per sistemi Windows e simili

Post n°49 pubblicato il **01 Settembre 2012** da exodus1984

Carissimi bloggers, rieccoci qui a spippolare come sempre i computer. :-))

Bene, oggi parleremo di nuovo di un ottimo sistema per il recupero delle immagini originali adatto soprattutto ad utenti Windows non molto portati con questo genere di procedure informatiche.

Da tempo volevo scrivere un articolo dedicato a questo stupendo sistema di recupero dati, ma non ne' avevo il tempo, ora spero che questo post possa essere davvero utile a chi cerca una valida soluzione semplice e veloce per il recupero e la riattivazione di sistemi Windows compromessi.

Redo Backup & Restore e' un piccolo sistema operativo in grado di aggirare tutte le protezioni che un disco fisso può' portare dovute alle installazioni di sistemi operativi Windows, e quindi come e' già' successo durante le mie precedenti assistenze informatiche, possiamo effettuare il backup di un'immagine Windows attivata e pulita, mettendola da parte magari su un disco fisso usb esterno per quando sara' necessario reinstallare tutto il sistema Windows.

Per usare questa distribuzione, dovrete prima scaricare la sua iso dal sito del produttore:

redobackup.org/download.php

Quindi dovete masterizzarla su un cdrom da 700 mega e di seguito inserirla nel lettore cdrom del computer di cui dovrete salvare una copia del sistema Windows che vi interessa.

Procediamo con ordine, il sistema RedoBKRK, deve essere fatto partire prima del boot iniziale del sistema operativo installato sul pc, e quindi dovrete entrare sul programma bios del computer andando nella sezione dedicata al boot, indicando che la prima unita' ad essere letta e usata sia proprio il lettore cdrom.

Salvate le impostazioni iniziali del bios(f10 etc...), inserite il supporto cdrom e fate riavviare il computer.

Alla prima schermata di RedoBKRK, selezionate la prima opzione del suo menu' iniziale, premendo il tasto "INVIO", il sistema si caricherà in memoria fornendovi una semplice interfaccia grafica su cui appariranno due pulsanti di attivazione: "Backup" e "Restore".

Per iniziare il salvataggio della nostra copia originale di Windows, clicchiamo sul pulsante "Backup", una veloce procedura identificherà per voi tutte le partizioni presenti su quel determinato disco fisso, chiedendovi in seguito di scegliere il disco/partizione di cui volete salvare un'immagine di backup.

Per i sistemi Windows, di solito e' sempre il primo disco fisso, oppure la prima partizione del primo disco fisso(installazioni standard).

Cliccate sul disco fisso scelto per il backup, e quindi sul pulsante "Next".

A questo punto, siete arrivati al passo 2, ovvero la scelta delle partizioni da includere nell'immagine finale, se Windows e' partizionato, vi conviene salvarle tutte per evitare problemi in seguito.

Dopo la vostra scelta, cliccate di nuovo su "Next", qui, siamo al passo 3, dove dovrete scegliere la destinazione finale della vostra immagine di backup, l'opzione attiva e' "Connected directly to my computer", che vi consente di utilizzare i dischi esterni usb per il salvataggio e il recupero, oppure potete scegliere l'opzione "Shared over a network", dove potrete caricare la vostra immagine disco su un server di vostra scelta.

Il passo 4 e' attivo solo se avrete inserito un disco esterno usb, qui potete crearvi una directory dove contenere i vostri dati di backup e quindi il sistema iniziera' a trasferire i dati completi dal vostro sistema Windows al supporto usb di salvataggio.

La velocita' di backup, dipende dalla quantità di dati che avete a disposizione e del tipo di hardware usato, in parole povere, se siete fortunati, ci vogliono 30-40 minuti per salvare un'immagine di Windows attivata e pulita(circa 18 giga...).

Detto questo, devo specificare che RedoBKRK, puo' scrivere su supporti formattati in modo diverso(fat32,ntfs, etc...) questo per consentire agli utenti il massimo vantaggio operativo mantenendo una semplicita' operativa davvero disarmante... ;-))

Ricordate solo questo, appena inserito il cdrom di RedoBKRK, dovrete avere gia' connesso il disco fisso esterno alla porta usb del computer, altrimenti, non trovando un drive per la destinazione dell'immagine finale, il programma si ferma perche' non puo' salvare i dati da voi richiesti.

Con RedoBKRK, abbiamo tool amministrativi molto utili, elenchiamone brevemente qualcuno:

Creazione di un disco bootabile RedoBKRK su key usb

Riparazione automatica del settore di boot(MBR)

Editor di partizioni (Gparted)

Utility disco, per montare supporti usb, formattare e smontare i dischi

Drive Reset, cancella tutti i dati dall'harddisk riportandolo alle impostazioni originali di fabbrica (pericoloso per utenti non esperti).

File recovery, per recuperare files cancellati dal disco fisso, basato su Photorec.

Quando avrete terminato il vostro backup/restore, RedoBKRK estrae il cdrom dal supporto e vi invita a riavviare o spegnere il pc premendo il tasto INVIO.

Ancora una volta, vi ricordo che i vostri dati sono importanti, per cui, se comprate un computer nuovo, attivate il vostro sistema Windows e poi fatevi subito il salvataggio del vostro nuovo sistema operativo, prima di iniziare a navigare su internet e a scaricare programmi, il 99 percento degli utenti Windows "normali", usa questo sistema con account amministrativo, percio' vi consiglio di creare almeno un utente con privilegi "standard", con il quale potrete andare su internet in modo "abbastanza" sicuro... ;-)))

Non fate come il mio parco utenti, che arrivano da me' tutti con la coda tra le gambe perche' il loro sistema Windows non parte piu', ricordate sempre di fare un backup del vostro sistema operativo funzionante, perche' poi le cose si complicano, infatti, molti utenti credono che il loro computer duri in eterno, mentre in effetti non e' cosi', e poi pretendono di reinstallare un sistema Windows attivato e funzionante senza copie di backup o supporti originali... :-(

In realta', poi si puo' recuperare quasi sempre il suddetto sistema, ma gli utenti dovrebbero imparare almeno le basi di una corretta manutenzione del sistema, Windows fornisce di default alcune piccole utility, anche se a volte non bastano a risolvere i problemi legati ad un uso sconsiderato del computer su internet, scaricando tonnellate di programmi di tutti i tipi... :-(

La durata media di un sistema Windows dipende da come viene utilizzato, dalla manutenzione che viene fatta dall'utente e da come quest'ultimo naviga in internet e dalla protezione scelta.

Nonostante questo, esistono migliaia di problemi che possono affliggere la durata di questi sistemi, per cui, il solo modo valido di tutelare i propri dati, e' quello di fare il backup totale del sistema funzionante, in modo da averlo sempre disponibile per eventuali problemi non sempre dovuti ai virus e al malware di rete.

Anche per oggi e' tutto cari bloggers, buon divertimento e buona navigazione a tutti voi. :-)

Riparare l'MBR su Windows e Linux

Post n°50 pubblicato il **03 Settembre 2012** da exodus1984
Carissimi bloggers, oggi parleremo di un piccolo sistema operativo in grado di recuperare l'accesso ad un sistema operativo compromesso da una mancata esecuzione corretta del settore MBR.

Andiamo subito a leggere il sito del produttore:

http://sourceforge.net/p/boot-repair/home/Home/

E quindi, scarichiamo l'immagine iso da masterizzare:

http://sourceforge.net/projects/boot-repair-cd/files/

Come possiamo leggere dalla descrizione, il suddetto sistema e' molto facile da usare, ha una licenza open GPL, puo' effettuare backup automatici, e come descritto, puo' recuperare l'accesso a molti sistemi operativi con MBR compromessi o che devono essere reinstallati.

Questo piccolo sistema operativo live, ci permette di riportare in vita un sistema Windows installato ma che non si avvia correttamente, dopo che l'utente proprietario-quasi-smanettone, lo ha leggermente spippolato...;-)

Analizziamo boot-repair-disk:

il suo menu' di boot e' configurato per sistemi a 32 e 64 bit, quindi dovrete scegliere la vostra architettura, fatto questo, premete il tasto INVIO sulla vostra selezione e il sistema iniziera' a caricarsi in memoria.

Quando il sistema sara' caricato, avrete a disposizione una stupenda schermata grafica con uno sfondo Hacker...:-)

Il sistema vi chiedera' di aggiornare, potete rispondere di no e proseguite, una veloce procedura fara' la scansione di tutti i dischi su quel particolare computer, facendovi accedere al menu' di configurazione di Boot-Repair.

Quando avrete riparato i guai al vostro MBR, potete dare un'occhiata al menu' principale di Openbox.

Clicchiamo su "Preferences" e scorriamo il menu' sottostante:

Boot-Repair:

ricrea il settore MBR e reinstalla grub anche su diverse partizioni per un boot particolare(diversi sistemi operativi su un solo disco).

OS-Uninstaller:

per ripulire vecchie installazioni di Windows e preparare il disco ad una nuova installazione pulita.

OS-Uninstaller cancellera' tutti i dati contenuti sul disco sotto manutenzione, formattando e preparando la partizione in formato NTFS, le opzioni sono: NTFS(fast), NTFS, EXT3.

Queste due principali utility, sono il cuore di questo piccolo sistema operativo, inoltre possiamo configurarci una connessione mobile nel caso ci siano degli aggiornamenti o semplicemente per navigare il web alla ricerca di soluzioni da poter adottare durante un'assistenza informatica.

Disponiamo di Iceweasel in versione 3.5.16, e del file manager PCManFM in versione 0.9.7 per la completa gestione del sistema in assistenza.

Detto questo, Boot-Repair-Disk svolge la sua funzione in modo assolutamente impeccabile, e quindi e' perfettamente consigliato portarselo dietro quando ci sono delle assistenze informatiche su sistemi Windows che devono essere svolte in modo particolare.

Cari bloggers, anche per stasera e' tutto, di nuovo a tutti voi una buona navigazione su internet e fate attenzione ai vostri sistemi Windows. ;-)))

Tecnologia e societa' moderna: la battaglia globale.

Post n°51 pubblicato il **14 Settembre 2012** da exodus1984

Carissimi bloggers, oggi vorrei parlare di questa societa' tecnologica.

Fin dagli albori della civilta', tutti gli esseri umani hanno cercato di vivere e sopravvivere in modi sempre piu' consoni ai loro bisogni.

Nella nostra societa', dopo millenni di evoluzione e progresso, ci ritroviamo come quando abbiamo iniziato il nostro percorso evolutivo, ovvero: siamo sempre in cerca di nuovi modi per sopravvivere.

Il progresso tecnologico e scientifico ci ha permesso di ottenere quasi tutto ciò' di cui abbiamo bisogno e anche il superfluo.

Questa societa' ci permette di sopravvivere solo dietro determinate regole imposte dall' economia globale, in cui una persona deve seguire il mucchio come una pecora segue il pastore.

L'economia globale, diventa in questo contesto, il punto centrale sopra cui gravitano interessi di ogni tipo, ma a pagare sono sempre i poveri diavoli che con il loro lavoro mantengono tutti questi carrozzoni creati ad arte da poche persone per guadagnare in modo "legale" i soldi dei risparmiatori.

A parte questo, la nostra societa' ha un disperato bisogno di cambiare, e il modo giusto per farlo, sara' di far prevalere i diritti dei molti contro quelli dei pochi che governano il mondo a loro esclusivo vantaggio.

La tecnologia oggi e' ovunque, e tende a prendere sempre piu' il controllo della vita e delle scelte che le persone fanno ogni giorno, a tutti gli effetti, noi ci riteniamo "liberi", quando invece non lo siamo affatto.

Esistono sistemi di intercettazione a livello globale e nazionale, il pensiero delle persone e' quindi svelato dai loro desideri espressi al cellulare, e subito accontentati da una casualita' davvero inaspettata... ;-))

La volonta' umana si puo' piegare ai voleri di poche persone preparate?

La risposta e': si!! Lo possiamo fare.

Nella psicologia applicata ad un semplice discorso, possiamo catturare la volonta' di una persona facendogli fare quello che in precedenza era stato preparato, in pratica, possiamo dire che le persone sanno farsi abbindolare anche se sono preparate a questo genere di cose.

Molte tecnologie sono state costruite dall'uomo per ingannare l'uomo, per ottenere il controllo di una persona o per controllare un'intera nazione, ma lo scopo di tutto questo, rimane sempre lo stesso: la sopravvivenza di una specie forte in rapporto ad una piu' debole, e quindi destinata all'estinzione.

La tecnologia che ci regala migliaia di giocattoli tecnologici che venti anni fa' ci potevamo solo sognare, questo mondo sempre piu' tecnologico, portera' all'estinzione della volonta' umana rendendoci tutti dei cyborg con gli stessi pensieri ed emozioni controllate da pochi esseri liberi che un giorno potrebbero essere i nuovi padroni dell'umanita'. :-)

Esistono tecnologie cosi' avanzate da far impallidire persino il controllo elettronico globale oggi esistente, ma il vero scopo di tutto questo discorso e' solamente questo, l'uomo deve controllare la tecnologia e non farsi controllare dalla tecnologia, se sapremo farlo, avremo a disposizione la cosa piu' bella che tutti credono di avere ma che in realta' non hanno: la vera Liberta', e non quella che abbiamo oggi, in questa societa' tecnologica che vuole tutto da noi, ma che ci fornisce solo quello che ci serve per poter mantenere questo stato di controllo elettronico globale. :-)

Cari bloggers, oggi ho mandato questo post per far capire alla gente la vera realta' in cui viviamo, anche se molti non lo sanno o fanno finta di non saperlo... ;-))

Come sempre, buona navigazione a tutti voi e buon divertimento (controllato) su internet. ;-))

Stagione di caccia 2012: possibile convivenza tra animalisti e cacciatori.

Post n°52 pubblicato il **16 Settembre 2012** da exodus1984

Carissimi bloggers, oggi tratteremo un argomento pungente sia per gli animalisti che per i cacciatori.

L'apertura della stagione di caccia, coinvolge da sempre molti aspetti diversi e nondimeno persone del tutto diverse, chi difende gli animali e chi paga una licenza per portarsi a casa la preda.

Chi difende gli animali ha le proprie ragioni, chi difende la caccia ha le sue, ma tutti quanti vorrebbero avere ragione escludendo la parte "avversaria".

La caccia, e' nata con l'uomo, e quindi per portare un po' di pace tra le parti si potrebbe dare ragione a tutti evitando polemiche continue che non portano mai a nulla.

Oggi, ho pensato ad una cosa davvero strana, ma che forse potrebbe essere utile per far "convivere" pacificamente le parti in causa, ecco la soluzione che si potrebbe adottare:

Abolendo la caccia, il giro d'affari che gli ruota intorno verrebbe distrutto, mettendo a rischio migliaia di posti di lavoro che forniscono licenze, armi, munizioni, mimetiche ed accessori vari.

Dalla parte opposta, il proliferamento incontrollato della fauna, porterebbe distruzioni alle coltivazioni, malattie trasmissibili all'uomo, costringendo prima o poi ad una decisione di "abbattimento forzato" della fauna interessata.

Detto questo, si potrebbe abolire la caccia per legge, mantenendo l'indotto delle armi e degli accessori e di conseguenza il mercato che gravita attorno semplicemente liberalizzando il mercato delle armi per la difesa personale, senza inutili visite mediche che non servono assolutamente a nulla.

Cosi' facendo, non si perderebbero posti di lavoro in questo settore, ma verrebbero addirittura creati nuovi posti di lavoro per le licenze, le armi e il giro d'affari sarebbe molto piu' elevato di quello che genera oggi il settore della caccia.

Inoltre, gli animalisti sarebbero accontentati e non ci sarebbero piu' inutili polemiche, se non per l'abbattimento forzato della fauna.

Cari bloggers, questa strana idea, mi e' venuta pensando alle leggi italiane in materia di difesa personale, per esempio: un delinquente vi entra in casa armato e pronto ad uccidere, voi non avete nessuna possibilita' di difendervi, perche' appunto il porto d'armi non viene concesso ai cittadini, mentre per i delinquenti e' davvero molto facile avere a disposizione armi e girare indisturbati senza che nessuno possa dire loro nulla, la liberalizzazione del mercato delle armi, porterebbe quindi alla creazione di milioni di posti di lavoro, i cittadini potrebbero difendersi e si ridurrebbe al minimo il mercato nero delle armi illegali, rendendo questo paese piu' sicuro e competitivo, inoltre abolendo la caccia per legge, tutti sarebbero contenti sia da una parte che dall'altra.

E con questo, anche oggi vi auguro una buona navigazione su internet e buon divertimento. :-)

La Grande Rete: chi sono gli Hacker?

Post n°53 pubblicato il **18 Settembre 2012** da exodus1984
Carissimi bloggers, oggi parleremo di un argomento che riguarda quasi tutti noi, ovvero gli Hacker e la rete.

La grande rete che ci ospita, ci da da vivere e ci fa morire, a volte non puo' bastare per tutte le nostre necessita'.

In questo contesto, esistono migliaia di esemplari umani(o quasi...) che navigano sui computer di altri utenti, a loro volta ignari di quanto stia succedendo sui loro sistemi.

La grandissima diffusione della banda larga mobile, ha contribuito a rendere questo fenomeno molto piu' vasto, infatti chi non possiede un cellulare al giorno d'oggi? ;-))

Quello che vorrei dire, e' che la gente comune che naviga su internet, viene solo informata dai media sui "disastri" combinati da presunti hacker, ma la verita' e' che la rete stessa e' stata creata da hacker e quindi la gente non dovrebbe credere a tutto quello che legge sui giornali al riguardo di hacker e simili.

Personalmente, conosco migliaia di hacker professionisti che lavorano per organizzazioni diverse a livello nazionale e internazionale, e fanno il loro lavoro per mantenere sicura e pulita la rete da elementi davvero distruttivi.

Tutte queste persone, garantiscono la disponibilita' della rete, per cui, tutti gli utenti dovrebbero ringraziare a questo proposito.

A parte questo, esistono davvero degli hacker che usano le loro conoscenze solo per distruggere la rete, magari con il favore di un governo nemico.

La grande rete, diventa a questo punto un terreno di scontri virtuali, dove vince sempre chi possiede una conoscenza superiore a quella del proprio avversario.

Nella "guerra virtuale" ci siamo dentro ogni giorno, ogni volta che ci connettiamo ad internet veniamo praticamente "bombardati" da pacchetti di dati di ogni forma e spessore, ma il 70% degli utenti "normali" non si accorge nemmeno di tutto quello che succede attraverso il protocollo di comunicazione della rete.

Siccome la sicurezza di rete non esiste, allora bisognerebbe istruire gli utenti, facendo capire loro il vero concetto di "sicurezza informatica", infatti, un antivirus puo' essere piegato al volere degli incursori virtuali, percui state attenti a cosa scaricate dalla rete, perche' esistono antivirus creati appositamente per fare il lavoro di un antiviurs, ma sotto la veste gratuita si nasconde quasi sempre un secondo fine.

Il firewall: tutti pensano che usando uno di questi programmi, ci si possa mettere al sicuro dai pericoli della rete, e invece.... ;-))

Prima che gli utenti possano installare un firewall, bisognerebbe insegnare loro a cosa serve, molti dei miei utenti, hanno scaricato alcuni firewall gratuiti dalla rete, ma hanno avuto piu' guai che con un esercito di virus mutanti...:-))

Questo fatto, implica che l'utente inesperto, scarica e installa di tutto e di piu' dalla rete, ma il programma poi deve essere configurato per offrire almeno una sicurezza di base... :-))

Concludendo, ci sono hacker "buoni" e hacker "K-attivi", ma il vero hacker sara' chi potra' aiutare davvero le persone, risolvendo tutti i problemi della rete e consigliando la corretta informazione sull'uso dei computer e dei programmi.

La rete e' il nostro "nuovo mondo", trattiamola bene e saremo ripagati con enormi soddisfazioni a livello personale e lavorativo.

Tutti gli utenti "non tecnici" vanno guidati verso il loro posto nel mondo virtuale, ho incontrato persone spregevoli che riparavano i computer in modo "gratuito", ma gli utenti non sapevano che il secondo fine era in agguato...(keylogger, backdoor, gabole varie...):-(

Cari bloggers, anche per oggi e' tutto, come sempre, buona navigazione a tutti voi e buon divertimento su internet.

Distribuzioni GNU/Linux: ultimi upgrade ai sistemi.

Post n°54 pubblicato il **20 Settembre 2012** da exodus1984
Carissimi bloggers, oggi mando solo un breve post per alcune distribuzioni GNU/Linux che possono interessare agli smanettoni di rete, andiamo ad elencarne qualcuna:

Slackware (sviluppo), la mia linux box preferita, incredibilmente bella e stabile se non la spippolate troppo... ;-)))

GeeXboX: media center, tv, musica, e molto altro per gli amanti del settore musicale/video.

Snowlinux: il "pinguino della neve"...:-) con tante nuove features per gli utenti piu' smaliziati... (non prendetevela troppo per il nome, che ricorda tanto il piu' famoso SnowLeopard prodotto dalla Apple).

Mandriva Linux: un sistema operativo che ha una lunga storia informatica e molti utenti si sono "fatti le ossa"(termine hacker...:-)) con questo sistema prima di lasciare definitivamente il loro amato Windows... :-) Ho ancora ben presente la devastante causa legale con la quale questo sistema fu' costretto a cambiare il proprio nome da Mandrake(tm) a Mandriva. A parte gli scherzi, il Mandriva Linux e' sempre stato un punto di riferimento per la sua facile gestione, e questo ha contribuito a "catturare" molti utenti dal parco MSWinz(tm) :-).

Tails: The Amnesic Incognito Live System, siamo alla release 0.13, con kernel upgradato al 3.2.23.

Di questa distribuzione, ne' avevamo gia' parlato in alcuni post precedenti, creata esclusivamente per la privacy dell'utente, ha bisogno pero' ancora di un po' di tempo per crescere e farsi conoscere meglio dal pubblico.

Tutto sommato, una delle migliori distribuzioni basate su Debian che rispettano quello che gli utenti sono, persone e non solo numeri nel traffico dati di internet.

Fedora: un fork del piu' antico e stabile linux, il Red Hat, progenitore di Mandriva Linux e di migliaia di altre distribuzioni derivate, usato prevalentemente nei sistemi server e worstations, ma apprezzato anche da un enorme parco utenti.

Cari bloggers anche per oggi e' tutto, augurandovi una buona navigazione, ci ri-leggiamo ai prossimi post :-)

Giochi numerici: Sfidiamo l'Europa con l' Euro Jackpot.

Post n°55 pubblicato il **23 Settembre 2012** da exodus1984
Carissimi bloggers, oggi proviamo a portare in italia l'Euro Jackpot.

Da qualche tempo, sono impegnato nella programmazione di un semplice sistema matematico in grado di prevedere le possibili colonne vincenti.

Esistono due programmi distinti, EuroJ e 2EU, rispettivamente in grado di determinare sia la possibile prossima uscita della colonna vincente dei principali 5 numeri richiesti, sia la cadenza dei 2 euro numeri richiesti per la giocata minima.

Ecco un semplice risultato di tutto questo, la giocata e' stata impostata su 5 schede da 2 euro ciascuna, i primi 5 numeri sono stati estrapolati dal programma EuroJ, mentre i restanti due, sono il frutto del calcolo con il programma 2EU.

La coppia EuroJ e 2EU lavora su un archivio completo di tutte le giocate effettuate dall'inizio del concorso.

Considerando che abbiamo a disposizione 12 categorie di vincite diverse, possiamo presumere la possibilita' reale di ottenere una vincita anche di portata elevata.

Ma ora basta con le spiegazioni tecniche, se volete provarci anche voi, ecco la selezione per il concorso di venerdi' 28 settembre 2012.

EuroJ					2EU	
37	41	26	44	16	6	1
34	24	27	20	19	4	3
5	22	26	46	8	2	8
40	39	2	32	5	3	5
36	21	4	31	24	7	2

Naturalmente, i numeri sono spesso traditori, e quindi, giocate il giusto senza esagerare, nonostante i programmi di calcolo che si avvicinano molto al jackpot siano abbastanza lineari, non sempre riescono a prendere la colonna vincente, benche' i numeri ci siano sempre tutti. :-)

Detto questo, cari bloggers, buona fortuna a tutti voi e come sempre, buon divertimento su internet. :-)

Racconti Hacker: la storia (infinita...) del progetto A.C.D.L.

Post n°56 pubblicato il **25 Settembre 2012** da exodus1984
Carissimi bloggers, oggi e' un giorno molto speciale, e quindi ho deciso di regalarvi uno dei miei libri elettronici creati con il progetto ACDL all'incirca diciotto anni fà. :-)

La storia del progetto ACDL(Ai Confini Della Legge) comincia nel lontano 1994, quando per la prima volta nella storia dell'informatica moderna, venne creata una raccolta di storie personali raccontate dai diretti interessati, ovvero gli hacker.

Da allora, sono cambiate moltissime cose nel settore informatico, e il progetto ha continuato ad esistere su server anonimi e criptati, ben lontano dal controllo globale che gia' allora faceva le sue vittime...:-)

Questo progetto, che altro non e' che una corposa raccolta di fatti, informazioni e situazioni personali raccontate e vissute dagli hacker dell'epoca, e' stato stampato in formato cartaceo nell'anno 2002 in cinquanta copie numerate e distribuite ai personaggi che raccontarono le loro avventure informatiche nella prima versione (ACDL versione 0.1.1).

Da tempo alcuni vecchi volponi di rete mi assillavano per rilasciare la versione 2.0, e cosi' e' stato, il tempo passato lontano dal blog, era dedicato totalmente a creare una nuova versione di ACDL per poterla portare anche sulla rete internet normale.

Cari amici volpini e volponi di rete, eccovi finalmente accontentati. :-)

La selezione dei capitoli in questo libro elettronico, e' molto modesta, in confronto alle informazioni contenute negli archivi del progetto, per la versione 2.0 di ACDL viene presentata una storia inedita, un racconto di avventura che ha lasciato letteralmente senza parole persino gli "addetti ai lavori" informatici piu' avanzati. :-)

Infatti, la versione distribuita per la rete ad accesso riservato(ACDL5ago2012.pdf) ha ottenuto nella prima settimana, un'utenza di circa duemila download al giorno. :-)

ACDL 2.0, e' stato reso disponibile dal 5 agosto 2012 su rete ad accesso riservato, la versione che e' stata portata qui su internet, e' invece disponibile dal 14 settembre 2012, e viene proposta al pubblico per la prima volta dalla creazione del progetto, viene rilasciata sotto CCPL versione 3, con alcune restrizioni adottate solo per la versione distribuita su internet.

Questa particolare opera e' dedicata a tutti gli utenti di internet e in modo speciale ai bloggers di Libero a cui piace leggere romanzi elettronici di avventura creati appositamente per il mondo virtuale in cui viviamo.

Come diceva un vecchio amico hacker: "Ogni leggenda di rete ha un fondo di verità...e noi siamo qui per trovare quella verità". :-)

La pagina web autorizzata per scaricarvi una copia certificata di questo libro elettronico, e' la seguente :

http://digilander.libero.it/exodus1984/

oppure, cliccando su "Sito" in alto a sinistra sul mio blog per accedere.

Il file .PDF e' ottimizzato per i tablet da 10 pollici, potete leggerlo su sistemi Android con diverse app scaricabili.

Un doveroso ringraziamento và al team di hacker che hanno concesso e autorizzato la pubblicazione di questa storia sulla normale rete internet, selezionandola e votandola direttamente dagli archivi criptati sul database del progetto ACDL.

Cari bloggers, a tutti voi auguro una buona lettura e come sempre, una buona permanenza su internet.

Giochi numerici: aggiornamento EuroJ e 2EU

Post n°57 pubblicato il **06 Ottobre 2012** da exodus1984

Carissimi bloggers, oggi vorrei proporvi una versione sperimentale dei programmi EuroJ e 2EU, creati alcune settimane fa' in tutta fretta per poter giocare ad Euro Jackpot.

Il programma EuroJ, estrae la possibile colonna vincente di cinque numeri tramite un database interno gestito da una funzione matematica complessa e creando un archivio di colonne vincenti grande circa 11giga, lo stesso lavoro, viene svolto dal programma 2eu, che puo'creare un archivio di euronumeri vincenti grande quanto quello del programma EuroJ.

Ecco un banale esempio del progetto EuroJ2012:

```
5f332d67901b06de88cd26fbb8872d41  2eu
19dff33a42eab42a77f003be0e34c3b7  2eu.c
81395911f900fae4e362f55a4a9a67be  2eu.exe
4f34a239aba8f394fa6779e322b22ed6  2eu.txt
7b1641f35ecd7233df35cfff4dce54be  euroj
1dfa06908559c2efeb612e8dacda4c50  euroj.c
746790fd444c5952b668d66378be8a7f  euroj.exe
424fb54a3234054a4d10e1c5f5a04e03  euroj.txt

-rwxr-xr-x  1 enrico enrico      690152  6 ott 09.42 2eu
-rw-r--r--  1 enrico enrico        1500  6 ott 09.41 2eu.c
-rwxr-xr-x  1 enrico enrico       22813  6 ott 09.41 2eu.exe
-rw-r--r--  1 enrico enrico 11811160388  6 ott 09.55 2eu.txt
-rwxr-xr-x  1 enrico enrico      690154  6 ott 09.26 euroj
-rw-r--r--  1 enrico enrico        1888  6 ott 09.24 euroj.c
-rwxr-xr-x  1 enrico enrico       22813  6 ott 09.30 euroj.exe
-rw-r--r--  1 enrico enrico 11166915188  6 ott 10.04 euroj.txt
```

I circa 22 gigabytes di archivio complessivo, contengono tutte le possibili colonne vincenti a partire dagli ultimi numeri estratti, il problema e' pero' ancora molto complesso, in quanto non sappiamo se una colonna vincente uscira' la prossima settimana oppure tra due mesi, in ogni caso, la funzione matematica genera tutte le colonne vincenti, anche se di fatto non possiamo certo giocarle tutte.

Un buon rapporto di gioco, e' il seguente, prendete le prime quattro colonne, abbinatele ai primi quattro euronumeri (2eu) e provate a giocare con questo sistema per almeno tre volte. Se dopo questo periodo non ottenete nulla, provate una nuova serie di colonne vincenti e di euronumeri.

I numeri ci sono sempre tutti, ma come ho detto in precedenza, il vero problema e' quello di mettere la colonna vincente al posto giusto e al momento giusto, infatti, se andiamo a controllare il database delle colonne vincenti estrapolate dal programma EuroJ, con una semplice ricerca troviamo subito la colonna vincente che e' appena uscita, confermando la bonta' della particolare funzione matematica usata per generare tutte le possibilita' offerte dal gioco.

A tutti gli effetti, i programmi sono molto validi per le previsioni del gioco, ma se avessimo la certezza che una colonna sara' vincente rispetto ad un'altra, vincerebbero tutti quanti mandando in fallimento EuroJackpot. ;-))

Non possiamo sapere in anticipo la colonna vincente che uscira' il prossimo venerdì, ma potete stare sicuri che sara' contenuta nel database di EuroJ gia' da questa settimana. :-)

Prevedere la futura colonna vincente e' un conto, ma saperla e giocarla in anticipo sarebbe davvero troppo bello... ;-))

Per cui, non affidate tutti i vostri risparmi a programmi di questo tipo, sicuri di vincere tutto e poi non vincete nulla...;-))

Ho creato questi programmi per verificare una mia personale teoria matematica al riguardo di EuroJackpot, e non con lo scopo principale di vincere il montepremi. :-)

Quindi, giocate il giusto senza esagerare, ma non fidatevi mai dei numeri, perche' sono traditori e beffardi in giochi di questo tipo. :-)

Come sempre, i programmi eseguibili li trovate nella mia pagina web, oppure cliccando su "Sito" in alto a sinistra sul mio blog.

Cari bloggers, augurandovi buona fortuna, ci rileggiamo alle prossime :-)

Computer Forensic: la stupenda distribuzione C.A.IN.E. (Computer Aided INvestigative Enviroment).

Post n°58 pubblicato il **13 Ottobre 2012** da exodus1984
Carissimi bloggers, oggi voglio parlare di un ottimo sistema operativo creato per il computer forensic, nè avevamo già parlato in precedenza, ma senza addentrarci nei particolari.

Come sempre, andiamo subito a visitare la pagina web del sistema operativo:

http://www.caine-live.net/

La distro in questione è C.A.IN.E.(Computer Aided INvestigative Enviroment).
Il bellissimo desktop, ci permette di navigare il sistema operativo in modo efficiente e rapido, possiamo impostare una veloce connessione internet mobile per trasferire i rapporti di consulenza informatica attraverso internet, usando la posta elettronica oppure creando il nostro rapporto con la CAINE Interface di livello grafico molto utile e veloce.

Il browser è Firefox in versione 15.0.1 (for Ubuntu),nella directory del DVD, troviamo il manuale operativo per comprendere meglio il sistema e le sue funzioni:

file:///usr/share/caine/Manual/index.html

I bash scripts Tools li trovate sotto questo percorso:

caine@caine:/usr/share/caine/pacchetti/scripts$

Infine, come si usa sempre, l'icona del Mounter deve diventare rossa per poter accedere in scrittura sulle key usb e supporti esterni, perche' questo e' un vantaggio informatico molto grande per questo tipo di distribuzioni, infatti, è tassativo montare i supporti sotto indagine in sola lettura, perche' così non vengono alterati dal sistema operativo che esegue l'ispezione dei dati per conto degli investigatori .

Il comando seguente imposta lo stato di READ-ONLY(verde)

```
root@caine:/home/caine# rbfstab -i
/usr/sbin/rbfstab first time run:
* Copying /usr/sbin/rbfstab to /usr/sbin/rbfstab
cp: `/usr/sbin/rbfstab' and `/usr/sbin/rbfstab' are the same file
* Creating udev rule /etc/udev/rules.d/fstab.rules
* Restarting udev service
udev stop/waiting
udev start/running, process 11565
Installation of /usr/sbin/rbfstab complete.
```

Il comando seguente imposta lo stato di WRITEABLE(rosso)

```
root@caine:/home/caine# rbfstab -r
removed `/etc/udev/rules.d/fstab.rules'
* Removed rbfstab rules from /etc/fstab
root@caine:/home/caine#
```

Dopo avere inserito la key usb, cliccate su "refresh" per vedere il vostro nuovo dispositivo sul sistema, e quindi selezionatelo con un clic di spunta sulla sua casella e cliccate il pulsante "OK" per confermare il mount del vostro dev usb.

Aprite il browser di file Caja, montate il vostro device e quindi selezionate con il tasto destro del mouse il menù "Scripts", quindi cartella "Admin" ed infine "Make Device Writeable", a questo punto ci appare un messaggio che ci informa di quello che stiamo per fare al nostro disco usb, ovvero renderlo scrivibile per copiarci il nostro rapporto da consulente informatico.

Questi sistemi GNU/Linux sono davvero belli e soprattutto utili, se siete investigatori informatici, consulenti governativi, ricercatori o altro, ma anche semplici utenti, imparare ad usare questo sistema significa capire le intrusioni informatiche, scoprire dati nascosti tra le immagini, e migliaia di altre gabole che ogni giorno il vostro computer rischia di prendersi perchè connesso ad internet, senza per questo chiedere la vostra approvazione.... :-))

Impostiamo ora una veloce connessione mobile usando questo sistema lanciato sulla memoria del nostro computer d'assalto, questo sistema non vi tocca il disco fisso e di conseguenza, nemmeno il sistema operativo che avete installato:

Sulla barra inferiore del desktop, clicchiamo sull'icona riportante i due pc-monitor, scegliamo quindi VPN Connections e di seguito Configure VPN.
Nella finestra che ci appare, abbiamo a disposizione tutti i tipi di connessione possibili, scegliamo "Mobile Broadband", clicchiamo sul pulsante "Add" per inserire i dati della nostra chiavetta internet e l'operatore telefonico.
Fatto questo procedimento, clicchiamo sui due pc-monitor presenti nella barra sottostante, e vedremo apparire il nome della connessione mobile che avremo dato al configuratore, clicchiamoci sopra e il modem si attivera'.

Cari bloggers, oggi mando questo post dal sistema C.A.IN.E. perchè stò verificando alcuni dati, ma presto potrò postare di nuovo dalla mia postazione di sempre, a tutti voi auguro un buon fine settimana non lavorativo, al contrario del sottoscritto che deve lavorare ad una consulenza informatica per lunedì mattina... :-(

Nuovi aggiornamenti GNU/Linux: le stupende distribuzioni della serie Ubuntu.

Post n°59 pubblicato il **19 Ottobre 2012** da exodus1984
Carissimi bloggers, oggi facciamo una breve recensione delle ultime distro della serie "Ubuntu". ;-))

Iniziamo velocemente con Ubuntu Studio, una variante della Ubuntu "standard", ma creata per i video, la grafica e il suono, come una espressione artistica personale, i creativi potranno sbizarrirsi davvero molto con questa distribuzione particolare, abbiamo a disposizione la versione per piattaforme I386 e AMD64.

Proseguiamo con la Edubuntu, una distribuzione creata per le scuole e per l'apprendimento, un ottimo sistema per imparare di tutto un pò, risparmiando tempo e denaro per le istituzioni scolastiche che sono già abbastanza messe male in Italia.... ;-))

Continuiamo con la Lubuntu, una distribuzione creata e progettata appositamente per poter riutilizzare i computer antichi con software di ultima generazione su internet(personalmente, ho resuscitato moltissimi vecchi cadaveri di computer usando questo velocissimo sistema...) .

Tra l'altro, questa distro usa un window manager progettato proprio per non succhiare tutte le risorse dei computer datati, LXDE e' un progetto ancora giovane, ma ha tutte le carte in regola per diventare uno dei migliori WM mai costruiti rispetto ai suoi fratelli più "pesanti" come Gnome e KDE.

Abbiamo poi la stupenda Xubuntu, con un window manager XFCE molto ben costruito e soprattutto testato e quindi con una stabilità anche maggiore rispetto al giovane progetto LXDE, bisogna dire che però, entrambi questi progetti, cercano di portare la funzionalità di applicativi diversi che un tempo potevano girare solo su Gnome o KDE, quindi la Xubuntu è molto valida per recuperare i vecchi computer che avete in casa, senza buttarli via perchè i sistemi Winzzz.... non ci riescono più a girare sopra... ;-))

Infine, troviamo la nuova Kubuntu con window manager KDE, adatta soprattutto ai computer di ultima generazione e workstation internet.

Come ultima, la Ubuntu di sempre con il desktop Unity, che ha suscitato tante critiche a livello di usabilità e preferenza degli utenti. Bisogna dire che però si possono usare anche tutti gli altri WM se questo di default non vi piace. :-)

Questi sono gli ultimi update ai sistemi Ubuntu del 18-10-2012.

Cari bloggers, anche per questa sera è tutto e come sempre, buon fine settimana a tutti :-)

Linux Day 2012: un appuntamento per conoscere e comprendere il fantastico mondo di GNU/Linux.

Post n°60 pubblicato il **21 Ottobre 2012** da exodus1984

Carissimi bloggers, oggi mando solo un breve post per ricordare agli amici smemorati che mi seguono solo via blog, che sabato 27 ottobre 2012 ci ritroveremo tutti quanti al LINUX DAY 2012.

A Gemona del Friuli ore 9.00-14.00, sabato 27 ottobre 2012 appuntamento con il pinguino.

Dopo un lungo anno di assenza, potremo confrontarci di nuovo sulle tematiche a noi più care, ovvero la strada della conoscenza, il futuro dei sistemi e della rete, la sicurezza informatica e tante altre cose che interessano il mondo del pinguino. :-)

E gli Hacker???? :-)) Vabbè, ci saranno anche loro, così accontentiamo tutti quanti. :-)

P.S.: per i volponi di rete che mi conoscono da sempre, quest'anno avrò a mia disposizione più tempo per poter rispondere a tutte le vostre domande, quindi non saltatemi addosso tutti insieme come fate di solito... ;-)))

Per eventuali contrattempi lavorativi da parte mia, seguite il blog per rimanere aggiornati.

Saluti a tutti quanti e buona domenica. :-)

Riflessioni personali: la mia pagina web, modifiche e pensieri vari :-)

Post n°61 pubblicato il **23 Ottobre 2012** da exodus1984
Carissimi bloggers, oggi sto riflettendo su alcune cose, e quindi visto che mi trovo in rete, tanto vale mandare un post sul blog... ;-)))

Cerco di costruire una semplice pagina web, utilizzando tutti i componenti che Libero ha messo a mia disposizione, ho un piccolo progetto per questo sito web, ma vorrei cercare di mantenere la pagina in questione più semplice possibile proprio perché il mio tempo è misurato con il contagocce, e anche se lavoro con i computer, non è sempre facile riuscire a bloggare qualcosa di buono e di interessante per gli utenti. ;-)

In queste settimane, ho programmato la pagina web qui su Libero in molti modi diversi, il tutto mirato ad ottenere qualcosa di utile non solo per la mia soddisfazione personale, ma anche per gli utenti occasionali che si trovano a passare nelle vicinanze della mia piccola pagina web. :-)

In passato, ho costruito siti web ben più grandi, ora invece, sembra che la mia soddisfazione sia quella di creare piccole cose, ma allo stesso tempo, dare anche un accenno di "professionalità" al sito personale.Infatti ho potuto constatare che sono più soddisfatto per avere creato una sola pagina web che un intero portale internet... ;-))

Tornare alle origini, dove il "poco" è bello e utile, al contrario di oggi dove il "troppo" finisce poi per essere del tutto inutile.Certe volte penso che dovrei mollare tutto, e fuggire su un'isola lontana, circondato dai miei libri e dai miei computer. :-)

Ma credo che questo, rimarrà un sogno come tanti altri, e intanto mi tocca lavorare... :-)))

Se volete dare un'occhiata alla mia pagina web. questo è l'indirizzo dove potete trovarla, anche se è ancora in costruzione(modifiche, spippolamenti, etc. etc.). :-)

http://digilander.libero.it/exodus1984/

Cari bloggers, anche per oggi è tutto, buona permanenza su internet a tutti voi. :-)

Preparativi per il Linux Day: il pianeta del Pinguino. :-)

Post n°62 pubblicato il **25 Ottobre 2012** da exodus1984

Carissimi bloggers, oggi facciamo i preparativi per il Linux Day, vabbè, non ci sta molta differenza tra una cosa e un'altra, ma l'importante è partecipare, almeno come sosteneva qualcuno.... ;-))

Bene bene, allora, il piccì portatile è pronto, gli strumenti d'assalto anche, manca solo una rispolverata al cervello e poi lo potremo ri-connettere alla realtà virtuale... ;-))

Cari bloggers e cari amici volponi che siete la mia "ombra" informatica, il 27 ottobre sarò a vostra completa disposizione per ben sei(6) ore, potete contattarmi dalle ore 9.00 alle ore 12.00, in seguito, vedremo per il pomeriggio. :-))

Dunque, dicevo, microregistratore d'assalto per la conferenza, macchina fotografica tattica per la foto di gruppo, computer portatile con connessione HSPA++ per reperire info su internet, naturalmente la testa sulle spalle con il relativo cervello(elettronico) innestato, e quindi possiamo partire per il Linux Day... ;-)))

Ecco il programma della giornata:

---

ore 9:30

Conferenza: Opensource come alternativa nel comune uso del PC, applicativi disponibili, migrazione a Linux

---

ore 10:30

Conferenza: Multimedialità con Linux

Install Fest: installazione guidata sui pc dei partecipanti

Conferenza: Linux e la nuvola: soluzioni libere

---

ore 11:30

Conferenza: la sicurezza in ambiente GNU-Linux

ore 12:30 - 14:00 pausa pranzo

---

ore 14:00

Install Fest: installazione guidata sui pc dei partecipanti (replica)

Conferenza: Strumenti di utilizzo quotidiano per l'amministratore

breve panoramica sugli strumenti basati su Linux per la gestione di un parco informatico di medie dimensioni.

Per info e mappe stradali: www.linuxday.it

Questo è tutto, un saluto a tutti voi e come sempre, una buona navigazione su internet. :-)

Linux Day 2012: un breve riassunto della giornata di oggi. ;-)

Post n°63 pubblicato il **27 Ottobre 2012** da exodus1984

Carissimi bloggers, in questo semplice post, cercherò di riassumere brevemente come è andata la seconda edizione locale del Linux Day di Gemona del Friuli.

Oggi è stata una giornata molto fruttuosa al Linux Day, benché la manifestazione fosse preparata per un pubblico non tecnico, ho avuto l'opportunità di imparare alcune cose in un modo diverso da come le conoscevo, quindi è davvero tornato utile andarci anche quest'anno. :-))

Il problema di questa manifestazione, è che bisognerebbe trovare un posto adeguato dove ospitare sia i computer che le persone, le due aule messe a disposizione dallo IAL di Gemona, sono bastate appena per contenere le varie conferenze e gli install-fest. :-)

In ogni caso, questa seconda edizione, ha portato la cultura del software libero ad un livello molto avanzato per alcune aziende locali intenzionate a dismettere un paio di licenze MS$$ in favore della GPL, e quindi abbiamo ottenuto un nuovo e valido obiettivo sul quale poter lavorare per le prossime edizioni. :-)

Visto ed appurato che molte piccole aziende artigianali cominciano ad utilizzare Linux più che altro per evitare i costi di licenza di programmi tipo Office-Win(MS$$$), e utilizzando programmi come Libreoffice per la gestione interna di fatture e bolle di spedizione, si potrebbe impostare una conferenza di carattere imprenditoriale che possa spiegare bene come usare al meglio questo prodotto in ambito aziendale.

Detto questo, impostare alcune conferenze specifiche sull'uso proprio del programma in questione, sarebbe molto utile per aumentare la conoscenza informatica di certe aziende locali che danno da vivere solo e sempre a MS$$$... e non degnano mai di uno sguardo il Pinguino più bello del mondo... ;-)))

L'aspetto interessante almeno per me in questa edizione del Linux Day, è stata certamente la conferenza sui programmi Opensource per la gestione delle biblioteche, ovvero: prestiti e resi, utenti e gruppi di utenti a cui inviare libri e gestione informatizzata di un server preparato appositamente per la gestione dei titoli, il server Kiwi e il gestore per biblioteche PMB usabile via Web, con una breve parentesi di confronto con il software BIBLIOWin 4.0 .

Infine, una soluzione più tecnica, ma sullo stesso piano free di PMB, è certamente il gestore Koha, mentre PMB dispone di un'interfaccia web un pochino diversa, in ogni caso tutti e due fanno bene il loro lavoro.

Ecco la pagina di Koha per il download:

http://koha-community.org/download-koha/

Mentre la pagina per scaricare l'ultima versione PMB si trova qui:

http://www.pmbservices.fr/download/index.php?lang=fr

Per quanto riguarda l'install-fest, è stato usato Suse Studio, che permette di creare dal proprio browser un intero sistema operativo Gnu/Linux creato in modo specifico per la macchina dell'utente finale, compilando tutto il software che si desidera avere a bordo del nuovo sistema, scaricandosi poi la relativa iso per masterizzarlo ed installarlo su macchine di uguale provenienza(recupero, rottamazione, etc etc.) :-)

Visto che conoscevo già Suse Studio, ho preferito seguire la conferenza sui software per biblioteche che per me era molto interessante e innovativo ad un Linux Day.

Eccovi il link se volete provare a farvi il vostro Linux su misura:

http://susestudio.com/

Cari bloggers, questo è un breve riassunto della giornata di oggi 27 ottobre 2012, come seconda edizione locale, è andata più che bene, e abbiamo molto materiale per prepararci bene per le varie conferenze durante il corso dell'anno fino al prossimo Linux Day. :-)

Numeri di Harshad e numeri cellulari: quello che gli utenti non sanno (parte 1)

Post n°64 pubblicato il **10 Novembre 2012** da exodus1984

Carissimi bloggers, oggi proviamo a giocare con i numeri.

Ma quali numeri direte voi? ;-))

Ma i numeri dei cellulari italiani naturalmente! :-)

Allora, prima di incominciare questo semplice post, devo premettere che ho condotto questo esperimento informatico al solo scopo di capire come stanno le cose, e anche per chiarire alcuni problemi che mi sono stati sottoposti da alcuni amici al riguardo dei loro telefoni cellulari, per costi elevati, o per spamming attraverso le proprie segreterie telefoniche.

Inizierò con la presentazione dei numeri di Harshad, che sotto certi aspetti, assomigliano molto ai numeri dei cellulari italiani se estrapolati da 0 a 9999999999 . :-))

Esistono siti web che calcolano e rendono pubblici i numeri di harshad e di conseguenza, qualche furbone ha provato ad usare quelle semplici liste di numeri associandole di fatto con prefissi e numeri cellulari italiani. :-))

Fin qui tutto bene, anche perché i numeri sono sempre numeri, ad esempio io posso scrivere il numero "100" e nessuno potrebbe reclamare per questo, ma se io scrivo "347XXXXXXX", allora vengo bastonato perché ho messo su internet il numero di un cellulare di qualcuno, questo è quello che succede quando un utente digita un numero di cellulare su Google e improvvisamente si ritrova su un sito in cui apparentemente, ci sono "liste" di numeri cellulari ma che con i cellulari non hanno nulla a che vedere...:-)

I numeri di harshad che vengono trovati da 0 a 9999999999 comprendono anche parecchi numeri che possono essere associati a dei cellulari, ma questa è solo una semplice ricerca matematica, infatti gli utenti che arrivano su questi siti web, si arrabbiano moltissimo perché trovano il loro numero di cellulare anche se ancora non lo hanno dato a nessuno... :-))

In seguito spiegherò come sia possibile trovare i "numeri cellulari" partendo da alcuni esempi pratici.

Il lavoro che ho condotto negli ultimi anni, mi ha fatto capire parecchie cose che potrebbero sembrare banali ai più, ma che se valutate sotto un altro aspetto, rivelano tutta la loro pericolosità per il portafoglio degli utenti cellulari.

Analizziamo ora alcune opzioni, la prima che mi è stata sottoposta, è molto chiara:

un amico mi contatta dicendomi che da diversi mesi viene regolarmente contattato da un numero sconosciuto che prima manda SMS non offensivi e poi, comincia a lasciare messaggi del tipo "respiro affannoso", "insulti di vario tipo".

Uno spammer cellulare, ma il problema non è questo, chi può' permettersi di chiamare degli utenti cellulari considerando il costo delle chiamate?

Bella domanda, allora visto che conosco abbastanza bene l'underground globale, decido di vestire ancora una volta i panni di Matrix e mi trasformo di nuovo in codice binario per valutare la situazione... ;-)))

A questo punto, non ci sono più dubbi, l'amico mi informa che il numero sconosciuto ha effettuato una ricarica non richiesta per il suo cellulare, e che qualche giorno dopo, ha lasciato un messaggio nella sua segreteria telefonica che diceva pressapoco così: "Sono un operatore XXXX, ho fatto una ricarica telefonica per sbaglio sul suo numero di cellulare, sarebbe così gentile da ricontattarmi?", l'amico, in buona fede, richiama il numero sconosciuto che gli fornisce i dati per effettuare una ricarica all'utenza che era stata "sbagliata" dal presunto "operatore telefonico", e qui scatta la trappola, il presunto operatore, non solo si riprende fisicamente i soldi della ricarica, ma il numero ricontattato dall'amico risulta essere a tariffazione speciale(3 euro scatto alla risposta + 3 euro per 1 minuto di conversazione sostenuto dall'amico per ridare indietro i soldi della ricarica "sbagliata").

Qualunque soggetto criminale può ricavare moltissimi profitti da questo genere di truffa, per cui se venite contattati da numeri sconosciuti sul vostro cellulare, la prassi è quella di non rispondere, perché come in questo caso esposto, il guadagno della truffa si attesta attorno ai 6 euro, che cresce esponenzialmente in base al numero di utenti contattati, come in questo caso, l'amico ci ha perso dei soldi, mentre il truffatore non solo ha riavuto la sua ricarica, ma ha anche guadagnato in tutto questo.

Che cosa ci insegna un caso del genere?

Ci insegna che il parco degli utenti cellulari è sempre più ampio, e quindi sempre più vulnerabile a truffe di questo tipo, basate sulla "buona fede" degli utenti.

In ogni caso, non mi sono fermato qui, e ho scoperto che esistono aziende "affiliate" a grandi nomi della comunicazione mondiale che mantengono liste di "numeri cellulari attivi" per operazioni di tele marketing cellulare.

Vedremo la prossima volta come operano queste aziende e come fanno ad avere i numeri dei nostri cellulari.

Un ultimo consiglio prima di salutarci, se venite contattati da un numero sconosciuto e non richiesto, mantenete sempre tutti gli SMS ricevuti e le registrazioni della segreteria telefonica come prova, vi serviranno sia per una eventuale denuncia contro il numero sconosciuto che come base di partenza per scoprire le intenzioni dei truffatori.

Se non siete tecnici informatici, potete contattare la Polizia Postale per chiarimenti in merito allo spam sul vostro cellulare. :-)

Come sempre, buona navigazione a tutti e buona domenica. :-)

Numeri di Harshad e numeri cellulari: quello che gli utenti non sanno (parte 2)

Post n°65 pubblicato il **11 Novembre 2012** da exodus1984
Carissimi bloggers, oggi proseguiamo l'analisi dei numeri cellulari, presentata nel post precedente.

Si era detto che bisogna stare attenti con le connessioni cellulari, e in parte è vero perché disponendo dei nuovi smartphone, ma anche di "antichi" cellulari, siamo sempre a rischio truffa, e cambiare numero per "essere al sicuro", non serve assolutamente a nulla come vedremo più avanti. :-)

Spiegherò poi come succede tutto questo, andiamo avanti un passo alla volta per ora, cercando di portare la conoscenza a un livello in cui tutti gli utenti possano comprendere, senza usare termini troppo tecnici.

Come promesso nel post precedente, oggi ci addentreremo in alcuni particolari definiti da qualcuno che conosco, "molto interessanti".

Iniziamo subito con una semplice analisi:

Gli utenti internet pensano di trovare informazioni sui numeri di cellulare nella rete, ma i database dei numeri sono di proprietà degli operatori di telefonia mobile che devono fare da garanti della privacy per i loro clienti.

I numeri che trovate su internet, e che sembrano numeri di cellulari, come spiegato in precedenza, possono essere di varia natura (sequenze harshad), ma anche liste di numeri a volte uguali a quelli dei vostri cellulari, ma che in realtà sono altre cose... :-)

Quando inserite un numero di cellulare in qualsiasi motore di ricerca, potete avere risultati diversi a seconda dello spider usato per l'indicizzazione dei dati nei siti web mondiali, ma questo, non vi farà avere certo le informazioni che cercate, in quanto un sito web che favorisce e pubblica numeri di cellulari con le relative informazioni di appartenenza del numero, è assolutamente illegale e pertanto può arrecare un serio danno ai clienti di un determinato operatore telefonico in termini di denaro e di affidabilità.

Questo ci porta ad una svolta nel nostro lavoro di ricerca, per capire come mai il nostro numero di cellulare sia finito nelle mani di qualche criminale informatico che crea e mantiene le cosiddette "liste attive".

Nel post precedente abbiamo analizzato un caso in cui una ricarica da 5 euro può fruttare ai truffatori 6 euro di guadagno, allora iniziate a capire a cosa servono le "liste attive"? :-))

Molto bene, queste liste, contengono nei casi più comuni i numeri di cellulare delle persone considerate in "buona fede" dai truffatori, ovvero persone che appunto in buona fede, richiamano il numero sconosciuto perché non vogliono avere debiti con nessuno, e pertanto si sentono in dovere di restituire la ricarica ricevuta per "errore" al loro numero di cellulare.

Richiamando il numero sconosciuto, avvengono alcune procedure particolari che rimangono "nascoste" agli occhi degli utenti in buona fede, vediamole insieme:

1) l'utente in buona fede richiama il numero sconosciuto per restituire i soldi della ricarica.

2) il numero di cellulare di questo utente, viene inserito nelle "liste attive" per un uso futuro da parte dei truffatori.

3) le "liste attive" vengono vendute a varie organizzazioni per effettuare a volte delle analisi di marketing, mirate a creare un parco utenti a cui vendere articoli vari, a questo proposito, vi posso dire che una buona parte di utenti cellulari accetta di buon grado sia SMS promozionali che chiamate dirette al proprio numero senza reclamare perché magari il prodotto offerto è per loro quello giusto...(vedremo poi le tecniche usate).

Ma la domanda iniziale che gli utenti si pongono è: come fanno ad ottenere un numero valido di cellulare??? :-))

I metodi sono diversi, ma tutti quanti sono mirati ad ottenere un numero attivo di cellulare, ne elencherò qui i più semplici per portare questa conoscenza ad un livello utile per gli utenti non tecnici.

metodo 1:

avete appena comprato lo smartphone dei vostri sogni, siete connessi su internet e state scaricando le varie app per vederle all'opera sul vostro nuovo cellulare:

non avete mai letto le richieste di installazione? Male...male per voi...:-)

Tutte le app, richiedono l'accesso diretto alla scheda telefonica e al numero di cellulare usato, e che mentre voi usate le vostre app, il vostro numero finisce tranquillamente su qualche server preparato proprio per questo scopo (sezione "liste attive" parte 1). :-)

metodo 2:

avete appena scaricato una nuova app che per voi potrebbe risultare utile, usando questa app, cliccate sopra un banner pubblicitario interno al programma e subito dopo, vi viene inviato un SMS in cui accettate l'abbonamento ad un servizio(non richiesto) al costo iniziale di 5 euro a settimana (sezione "liste attive" parte 2). :-)

Metodo 3:

accettate di confermare un SMS che per voi risulta uno sbaglio nel numero di cellulare e pensate che forse era diretto ad un altro utente:

messaggi di auguri da un presunto parente, e quindi inviate un SMS dal vostro cellulare per informare quell'utente che ha sbagliato numero. (sezione "liste attive" parte 3). :-)

Poi, esistono migliaia di altri metodi vari con cui ci si può impossessare di un numero valido e attivo, ma che non verranno spiegati per non dare la possibilità agli spammer che leggono questi articoli di arrecare un ulteriore danno agli utenti dei cellulari.

Nei prossimi post, parleremo delle "liste attive", di come vengono create e gestite al solo scopo di informare gli utenti cellulari del mondo oscuro che esiste dietro una "lista attiva" di numeri. :-)

Come sempre, buona navigazione a tutti e buona permanenza su internet.

Numeri di Harshad e numeri cellulari: quello che gli utenti non sanno (ultima parte)

Post n°66 pubblicato il **12 Novembre 2012** da exodus1984

Carissimi bloggers, oggi parleremo delle "liste attive" e di come possono essere usate per manipolare i numeri cellulari al solo scopo di chiarire alcuni aspetti che possono essere usati per truffare gli utenti.

Come ogni mio post dedicato a questi argomenti particolari, ribadisco le mie intenzioni di studio e conoscenza che mi hanno portato a creare un programma che servirà per far comprendere agli utenti come accadono queste cose.

Premetto inoltre, che qualunque soggetto, anche dotato di scarse qualità di programmatore, sia perfettamente in grado di crearsi un intero database di numeri telefonici, appartenenti ad ogni operatore italiano noto, presente e futuro, da questo semplice programma, capirete in seguito il perché di quanto cambiare il vostro numero abituale con uno nuovo e non ancora distribuito ai vostri amici, sia perfettamente inutile.

Questa breve presentazione, ci servirà in primo luogo a capire come si possono ottenere i numeri di cellulare di ogni operatore italiano, mentre in secondo luogo, il suddetto programma, ci consentirà di capire come vengono utilizzate le cosiddette "liste attive", fornendo a tutti gli utenti una semplice base di conoscenza al solo scopo di creare un comportamento corretto per gli utenti cellulari di fronte a sfide come queste. :-)

Molto bene, chiarito lo scopo di questo programma, ora andiamo a vedere che cosa può fare nella realtà, ricordate il primo post in cui mi trasformo in Matrix e divento codice binario? :-)))

Ok !!

Il suddetto programma, serve proprio per creare un database di numeri che in questo test informatico ci servirà a capire come vengono usate le "liste attive".

Cercherò di essere molto semplice e conciso nel presentarvi il banale codice sorgente che serve al nostro scopo, e che di fatto, ci fornisce tutti i numeri di cellulare che ci possono servire per la nostra ricerca della verità a livello matematico:

```
@load(loadDB(prefissicell.txt));
selfcreate(@load);
 filegen(@load);
```

Questo è tutto quello che ci serve per avere a disposizione l'intero archivio dei numeri cellulari con il prefisso di ogni operatore mobile italiano.

Ma la cosa non finisce certo qui, inserendo i prefissi mondiali di tutte le reti cellulari estere, abbiamo a disposizione il database numerico globale di ogni utente cellulare del pianeta, in pratica, possediamo tutti i numeri cellulari disponibili in ogni parte del mondo. :-)

Cari bloggers, avete capito adesso quanto sia semplice trovare tutti i numeri di celluare?

Certo, trovare i numeri è una cosa molto semplice ma non lo è sapere a chi appartengono, infatti questo semplice programma, è il culmine della nostra ricerca matematica e ci permetterà di comprendere come e perchè vengono usati i numeri dei telefoni cellulari a nostro danno.

Questa è una semplice ma efficace tecnica adottata da molte unità di intelligence e usata per anni da alcuni hardware strategici proprio per il controllo globale delle comunicazioni cellulari.

Va bene, lasciamo perdere i servizi segreti e le tecniche di spionaggio globale e veniamo subito al sodo, avevo promesso di non essere troppo tecnico per poter portare la conoscenza anche agli utenti che non comprendono nulla di programmazione, ma dovevo presentarvi questo codice per potervi spiegare il suo

funzionamento al fine di arrivare a comprendere come funzionano alcuni tipi di truffe basate sui numeri cellulari.

Inizierò a spiegare questo semplice programma:

l'istruzione @load carica in memoria un semplice file di testo che contiene

tutti i prefissi di tutti gli operatori italiani:

```
@load(loadDB(prefissicell.txt));
```

L'istruzione selfcreate(@load); genera gli archivi di numeri, un archivio per ogni prefisso trovato nel file prefissicell.txt.

```
selfcreate(@load);
```

Infine, l'istruzione filegen(@load); deposita su disco fisso tutti gli archivi dei numeri generati da selfcreate(@load); con il nome del rispettivo prefisso cellulare come nome di file(330.txt, 347.txt etcetc...).

```
filegen(@load);
```

Ora, vedremo insieme che cosa viene creato dal programma, prima una directory da 3,4 GB che contiene a sua volta delle sottodirectory, le quali contengono a loro volta tutti i numeri possibili usati per ogni singolo prefisso cellulare italiano. :-)

```
enrico@exodus84:~/celltest9$ ls

database_cellulari_italiani prefissicell.txt src Makefile

enrico@exodus84:~/celltest9$ cd database_cellulari_italiani
enrico@exodus84:~/celltest9/database_cellulari_italiani$ ls -la

drwxr-xr-x 9 enrico enrico 4096  9 nov 22.10 .
drwxr-xr-x 6 enrico enrico 4096  9 nov 22.35 ..
drwxr-xr-x 2 enrico enrico 4096  9 nov 22.08 CoopVoce
drwxr-xr-x 2 enrico enrico 4096  9 nov 22.10 PosteMobile
drwxr-xr-x 2 enrico enrico 4096  9 nov 20.53 TIM
drwxr-xr-x 2 enrico enrico 4096  9 nov 21.07 TRE_H3G
drwxr-xr-x 2 enrico enrico 4096  9 nov 22.04 UNOMobile
drwxr-xr-x 2 enrico enrico 4096  9 nov 21.26 VODAFONE
drwxr-xr-x 2 enrico enrico 4096  9 nov 21.52 WIND
```

Vediamo in dettaglio il prodotto interno di un archivio:

enrico@exodus84:~/celltest9/database_cellulari_italiani$ cd WIND

enrico@exodus84:~/celltest9/database_cellulari_italiani/WIND$ ls -la

-rw-r--r-- 1 enrico enrico 110000068 9 nov 21.48 320.txt

-rw-r--r-- 1 enrico enrico 110000068 9 nov 21.48 323.txt

-rw-r--r-- 1 enrico enrico 110000068 9 nov 21.48 327.txt

-rw-r--r-- 1 enrico enrico 110000068 9 nov 21.49 328.txt

-rw-r--r-- 1 enrico enrico 110000068 9 nov 21.49 329.txt

-rw-r--r-- 1 enrico enrico 110000068 9 nov 21.49 380.txt

-rw-r--r-- 1 enrico enrico 110000068 9 nov 21.49 383.txt

-rw-r--r-- 1 enrico enrico 110000068 9 nov 21.49 388.txt

enrico@exodus84:~/celltest9/database_cellulari_italiani/WIND$ du -h *

106M 320.txt

106M 323.txt

106M 327.txt

106M 328.txt

106M 329.txt

106M 380.txt

106M 383.txt

106M 388.txt

Come potete vedere, ogni singolo archivio creato da questo banale programma, contiene al suo interno circa 10 milioni di numeri disponibili, se sommiamo il contenuto di tutti i numeri per tutti gli operatori, otteniamo la bellezza di circa 330 milioni di numeri a disposizione per la sola rete cellulare italiana, e se proviamo ad eseguire una semplice ricerca di un numero cellulare, lo troveremo senza alcuna possibilità di commettere errori.

Ogni singolo archivio può essere letto tramite un comune editor di testo, e aperto in memoria occupa circa 1,4 Gb, nelle prove precedenti a questa, ho mandato in DoS(Denial of Service) il sistema di generazione dei numeri caricando in memoria un file di testo da 20 Gb per valutare la complessità di questa operazione.

Infatti, avendo a disposizione un vecchio pc intel I7-960 con a bordo solo 12 Gb di memoria ram e uno swap di 23 Gb, sono riuscito a piantare di brutto anche questo sistema Linux...:-(

La ricerca matematica dei numeri cellulari può aprire molte porte sul sentiero della verità, ma purtroppo a farne le spese come in questo caso, sono i nostri amati computer... :-)

Riparati quindi gli errori di spippolamento dovuti alla mia particolare natura informatica, ho potuto concludere questa ricerca in modo ottimale, e, dati alla mano, ho finalmente potuto soddisfare alcune questioni importanti in merito all'uso indiscriminato dei numeri di cellulare, accontentando di fatto gli amici che hanno cercato un aiuto per i problemi dovuti all'uso dei cellulari.

NOTA IMPORTANTE:

Va comunque chiarito che in tutti questi archivi sono contenuti solamente i numeri generati dal suddetto programma, e non le informazioni degli utenti associati ai numeri, che in quanto riservate, sono a disposizione dei soli operatori telefonici e delle forze dell'ordine per le loro indagini sui tracciati cellulari.

In realtà, devo ammettere che forse, mi sono spinto ad un livello anche troppo avanzato, e forse non tutti gli utenti di questo blog potrebbero comprendere il valore reale di questa mia personale ricerca matematica, in fondo, trovare certe verità, significa anche saper portare la conoscenza ad un livello utile per tutte le persone, in questo caso, questa ricerca è stata fatta per aiutare alcuni amici in difficoltà con i loro telefoni cellulari.

Questo ci riporta subito al tema del presente post, ovvero: le "liste attive".

Come ho spiegato nei post precedenti, queste liste vengono create partendo sempre da un banale programma come questo, che prepara un set di numeri a cui di volta in volta vengono aggiunti i dati catturati dagli spammer cellulari. Effettuato questo lavoro, le liste possono essere vendute, aggiornate e usate da qualsiasi persona che sia in grado di usare un editor di testo. :-)

Quindi, se ricevete chiamate cellulari da numeri a voi sconosciuti, la cosa più saggia da fare è proprio non rispondere ne alle chiamate, ne agli SMS, e se il numero sconosciuto continua ad infastidirvi senza rivelare la sua identità, state pur certi che si tratta di un tentativo per estorcervi qualcosa oltre che mettere il vostro numero cellulare su una lista attiva.

Cari bloggers, con questo post concludiamo la serie dedicata ai numeri cellulari e alle loro applicazioni truffaldine nei confronti degli utenti in buona fede.

Spero che questi semplici post possano far aprire gli occhi a molti utenti che ritengono il proprio numero di cellulare "al sicuro"... ;-)))

Inoltre, potete capire benissimo da questi esempi come sia inutile per tutti noi cambiare il nostro numero di cellulare con uno nuovo e sconosciuto a chi ci perseguita, verrete sempre ritrovati, e non potrete sfuggire in ogni caso al controllo globale...(oppure si...?) 8-)))

Come sempre, buona permanenza su internet e buona navigazione a tutti voi. :-)

Sistemi operativi Android: hardware MK808 e MK802

Post n°67 pubblicato il **19 Dicembre 2012** da exodus1984
Carissimi bloggers, oggi impareremo ad usare un piccolo dispositivo Android che farà la felicità dei pantofolai televisivi... ;-))

Inizierò questa breve presentazione dicendo che il dispositivo da me testato oggi, si è rivelato davvero interessante sotto molteplici aspetti.
Il "giocattolo" in questione altro non è che il dispositivo MK808, che monta una cpu Rk3066 dual-core, con clock da 1.2 a 1.6 Ghz (Cortex A9).

Vediamo insieme le principali caratteristiche tecniche del dispositivo:

1 GB di ram ddr3
espansione in formato micro-sd T-flash da 32GB
wi-fi 802.11 b/g/n
sistema operativo Android 4.1 - flash 11.x - html5
dimensioni: 88x31.5x15.8
peso: 50 grammi

prezzo internet: 74.68 Euro

Dunque, la prima cosa da fare è quella di aprire la confezione e controllare se sono disponibili i cavetti per la connessione di base al proprio TV tramite porta HDMI.
Preparate tutte le connessioni per il primo boot del sistema, ho usato un semplice mouse, la tastiera non serve, ma sarebbe utile averla, almeno per me che sono abituato a scrivere programmi e documentazione varia... :-)

La prima cosa che dovete fare è configurare il menù impostazioni e settare il sistema operativo per la lingua italiana, fatto questo, se disponete di un router wi-fi, potete usare il codice PIN(Wps) oppure se avete il pulsante WPS a livello hardware per poter connettere il dispositivo ad internet.
Se invece volete fare gli smanettoni come il sottoscritto, andate a configurarvi a mano la vostra connessione al router, e potrete scoprire molti particolari con il rilevamento delle reti wireless. :-)

Come consiglio principale, vi posso dire che dovrete rilevare il MAC address della scheda di rete dell' MK808, al fine di poterlo inserire all'interno del filtro MAC del vostro router.
Per il rilevamento del MAC di dispositivo, dovrete accedere all'applicazione "Impostazioni" presente di default sul desktop, quindi attivare il wi-fi portando il selettore su "on", attendere l'attivazione della rete e quindi cliccare in alto a destra dove si trovano i tre(3) quadratini uno sopra l'altro e passerete al menù di gestione wi-fi.
Su questo menù, cliccate su "avanzate" e potrete scoprire il MAC del vostro dispositivo android. :-)
Se avete il controllo delle connessioni sul vostro router internet, dovrete inserire qui il numero MAC del dispositivo, per permettergli di connettere la vostra rete interna e di conseguenza potersi connettere ad internet. :-)

Oggi ho testato questo piccolo dispositivo su internet, e il risultato è stato davvero sorprendente, devo dire che già parecchi anni fà avevo visto dei server internet grandi quanto una scatola di fiammiferi che giravano su sistemi operativi GNU/Linux, percui, questi dispositivi non sono affatto nuovi per me, ma hanno portato una ventata di novità per chi non li conosce ancora e giustamente, molti amici informatici sono rimasti stupiti di quello che può fare questo piccolo dispositivo Android.
Da parte mia, non vedo l'ora di mettere come si dice, le mani "in pasta", ovvero iniziare uno spippolamento a largo raggio di questi dispositivi al fine di capire che utilizzo si potrebbe fare di un dispositivo del genere eliminando come sempre l'uso per cui è stato progettato, trovandogli una nuova collocazione nel mio panorama informatico... :-)

Nei prossimi giorni, vedrò di cominciare a fare alcune modifiche alla versione "antica" di questo dispositivo, ovvero l'MK802, che monta un processore AllWinner A10 con clock da 1 Ghz (Cortex A8).

Usare il televisore di casa per navigare su internet non è certo una cosa nuova, ma farlo con un computer che contiene un hardware di questo tipo, risulta davvero entusiasmante, anche per uno come me che il televisore lo usa solo come maxischermo per i computer di casa... :-))

Allora, concludendo questo post sui sistemi hardware Android, vi consiglio di munirvi di una tastiera bluetooth che contenga anche un touchpad se non avete intenzione di usare un mouse BT separato, per lo storage dei vostri files, potete connettere un disco fisso esterno tramite HUB Usb, e crearvi così una veloce postazione internet senza staccarvi dal vostro amato televisore da 32 pollici... :-))
La navigazione è molto fluida e possiamo scaricare tutti i browser che ci piacciono dall'app store.

Con questo, cari bloggers, un augurio di buone feste a tutti quanti e naturalmente, per tutti gli smanettoni, un grandioso spippolamento sia hardware che software e un buon divertimento su internet. :-)

Sistemi Operativi: breve guida alla configurazione per MK808

Post n°68 pubblicato il **22 Dicembre 2012** da exodus1984
Carissimi bloggers, oggi impareremo a configurare il dispositivo MK808 per renderlo adatto al nostro tipo di navigazione personale.

Per una corretta configurazione dei dispositivi, si rende necessario un account e-mail sui server di Gmail, questo account serve per l'accesso al play store, per poter scaricare e installare le applicazioni che ritenete utili.

Ecco un breve esempio di configurazione per un account Gmail da usare per i nostri test su questi dispositivi Android:

Dal desktop del MK808, cliccate sull'icona "impostazioni", dal pannello principale dell'applicazione, dovete portarvi sulla scheda "account", e da questo punto in poi cliccate sulla dicitura "+ Aggiungi account".

Ora disponete di una nuova finestra che contiene le tipologie degli account possibili per questo mini-sistema, quindi, se come abbiamo detto in precedenza, avete già un account sui server di Google e ritenete opportuno usarlo per questo dispositivo, allora da questa finestra cliccate su "Google", ed arriverete ad un form che vi chiederà se volete creare un nuovo account oppure usarne uno esistente, clicchiamo su "Esistente" oppure su "Nuovo" nel caso vi serva un nuovo account.

Questo account, vi serve anche come nuovo indirizzo di posta elettronica, che verrà utilizzato per accedere al play store per libri, applicazioni, giochi e varie altre cose che vi potrebbero essere utili.

Passiamo ora alla configurazione successiva di data e ora:

spuntate la casella del settaggio di "Data e ora automatiche", verranno usati la rete e i time server per mantenere aggiornato il vostro dispositivo in modo sincrono con i server della rete, backup compreso.

Selezioniamo adesso il fuso orario e impostiamolo su "GMT+01:00, Ora Standard Europa Centrale", quindi spuntiamo la casella su "Usa formato 24 ore" per ottenere l'ora del tipo 14:30 invece che 2:30.

Il formato della data può essere scelto tra quattro(4) diversi tipi di formato internazionale, selezioniamo per il nostro uso il formato "Regionale 22/12/2012".

Visto che ho testato per quasi tre giorni questo dispositivo, ho commesso un sacco di errori vari mirati a comprendere le potenzialità e i difetti di questo sistema, e ho concluso che è molto utile per navigazioni "improvvisate" su internet, tenendo conto che il mini pc, non disperde calore e le sue prestazioni possono migliorare se tenuto costantemente acceso e operativo sul vostro televisore.

Per cui, quando connettete questo dispositivo al TiVù, sul telecomando dello stesso, premete il tasto "source" per selezionare l'entrata del segnale che desiderate, in questo caso l'HDMI(1,2,3,4,5) a seconda del tipo di televisore che avete in dotazione.

se commettete errori gravi di spippolamento software del dispositivo, ci viene in aiuto il settaggio "Ripristino dati di fabbrica", se cliccate qui sopra, il sistema ritornerà alle impostazioni originali di fabbrica, ma questo non è un backup, ma solamente un ripristino della macchina, infatti questa funzione, vi cancella tutti i settaggi, gli account email, facebook etc.. che avevate impostato, oltre che tutte le applicazioni che avevate scaricato, in pratica, dovrete riconfigurare di nuovo lingua, rete, mail,account e ri-scaricarvi di nuovo tutti gli aggiornamenti che avevate fatto prima.

Una nota, se avete sincronizzato un backup quando il sistema vi è andato in tilt, ritornerete ad avere sempre gli stessi errori, infatti il reset hardware, serve proprio a questo scopo, ovvero ripartire con un sistema pulito e semplice come quando è uscito di fabbrica.

Per cui, considerate se avete bisogno di un backup oppure se ritenete il caso di effettuare un reset totale del dispositivo.

Nel mio caso, il backup mi ha ricaricato gli stessi errori, e quindi ho preferito ripartire da zero con il dispositivo riconfigurandolo diverse volte per le valutazioni finali.

Passiamo adesso ad una breve panoramica del supporto rete dell'MK808, sul menù "Wireless e Reti", clicchiamo su "Altro...", ora avrete a disposizione tutto quello che vi serve per configurare diversi tipi di connessione tra cui:

VPN

Hotspot portatile

Reti Mobili

PPPoE

ognuno di questi settaggi meriterebbe un post a parte, ma ogni utente di questo dispositivo possiede quasi sempre connessioni internet differenti e quindi sarebbe oltremodo inutile addentrarci all'interno di questi argomenti che sono già disponibili su internet alla portata delle ricerche di qualsiasi utente che ne voglia sapere di più.

Dalla mia personale analisi di queste funzioni, ho ottenuto diverse informazioni atte a costruire un nuovo dispositivo basato sempre su questa tecnologia ma ancora più avveniristico. :-)

Per esempio prendiamo un HUB usb con sole quattro porte, una per la tastiera, una per il mouse, una per il disco fisso esterno e una per la video conferenza, che cosa ne pensate? Naturalmente il tutto contenuto nelle giuste dimensioni, risulta un giocattolo ottimale da portarsi dietro nei ritrovi degli smanettoni e nei vari LinuxDay... ;-))

Cari bloggers anche per oggi è tutto, buone feste a tutti quanti. :-)

Sistemi operativi Android: guida al dispositivo MK802/2

Post n°69 pubblicato il **23 Dicembre 2012** da exodus1984

Carissimi bloggers, oggi parleremo della configurazione iniziale di un altro piccolo dispositivo, l'MK802/2.

Questo dispositivo, monta di serie il sistema operativo Android 4.0, con le sottostanti principali applicazioni per l'uso per cui è stato costruito:

Youtube, Twitter, Angry Birds, Office, Gmail, Skype

Il chip principale è un AllWinner A10 da 1 Ghz, cortex A8, il processore grafico montato a bordo del dispositivo è un AMD z430 e AMD z160 da 27M Tri/sec.

Il network è basato su un protocollo wireless 802.11 b/g/n WAPI (Ralink 8188), mentre il supporto per la tastiera, è il classico 2,4 Ghz, mouse compreso.

La portata del segnale in interno, è di 30 metri, ma dalle prove effettuate, il risultato non è certo dei migliori, quindi credo che i 30 metri dichiarati, possano intendersi in uno spazio abitativo libero da muri in cemento armato anche dello spessore di 10-15 centimetri, sufficienti ad abbattere la trasmissione e la ricezione di questo dispositivo ad un semplice 20-25% delle dichiarazioni del manuale tecnico.

La tensione di alimentazione, viene fornita da un cavetto USB, fornito a corredo, che può essere collegato ad una presa USB del televisore per le prove che vorremo fare, ma che altrimenti, consiglio di sostituire con un alimentatore da rete elettrica 220V che disponga di una uscita usb per poter pilotare al meglio il nostro dispositivo Android.

Questi alimentatori USB, li potete trovare ovunque, e se comprate tutto su internet, ancora meglio per voi... ;-))

Le dimensioni di questo dispositivo Android, sono circa 100x30x12 mm, disponiamo di una fonte in ingresso del tipo mini-usb per la sua alimentazione(5V 1A), di seguito, abbiamo un'entrata usb Host per il trasferimento dati diretto al dispositivo, ed inoltre una porta micro usb per i device che vorrete installarci sopra in futuro.

Per il primo boot di questo tipo particolare di dispositivo Android, dovete connettere come già spiegato prima, la porta micro usb dedicata alla sua alimentazione, quindi inserire il cavetto HDMI nella porta specifica del vostro televisore e quindi selezionare con il telecomando dello stesso la fonte di segnale in entrata per predisporre il vostro televisore al primo boot del sistema.

La configurazione, come spiegato anche per il dispositivo MK808, viene effettuata solo con il mouse collegato alla porta usb, mentre il sistema operativo Android ricrea una tastiera virtuale sullo schermo che può essere usata dal mouse fisico connesso al dispositivo.

Il boot del sistema Android 4.0, viene effettuato in circa 10 secondi, ma sarà compito dell'utente aprire le applicazioni e farle risiedere in memoria per un accesso ancora più veloce, durante i miei test, il sistema è risultato molto più reattivo dopo quattro giorni di accensione continua e con le applicazioni sempre pronte e aperte in memoria.

Come consigliato nei post precedenti, anche per questo dispositivo si rende necessario un account di posta elettronica, reperibile come sempre sui server di Google per i vostri test, ma anche per accedere al market applicativo fornito da Google e da altre società, a questo scopo, farete bene a controllare la spunta sul menù "impostazioni", che essendo abilitata, vi permette di installare qualsiasi cosa, malware compreso, per cui, scegliete bene quello che vi serve davvero dal market Android o dovrete resettare il vostro dispositivo per ritornare al sistema originale...;-)

Ci sono alcune considerazioni da fare in merito alle applicazioni, per esempio, prima di installare qualche app che vi interessa, leggete bene le sue indicazioni, ovvero: per sistemi cellulari, se vanno bene anche sui tablet, in ogni caso, avete a disposizione la regolazione dello schermo del televisore nel caso vogliate installare una app per schermi di cellulari, che sul televisore potrebbe rendervi la visione difficoltosa o addirittura bloccare temporaneamente il sistema, in questo caso un reset della memoria attiva, riporterà il sistema al suo funzionamento normale liberando la ram in pochi secondi.

Infine, per concludere questo breve post, ribadisco la necessità di usare sempre un backup, se avete applicazioni importanti e dati che non volete perdere, quindi una key usb da 4/8 Giga dovrebbe essere sufficiente a contenere quasi tutto il vostro prezioso materiale informativo...:-)

Anche per questo dispositivo abbiamo il reset per riportare il sistema ai parametri impostati in fabbrica, ma non usatelo se non sapete bene quello che state per fare, il mio consiglio in questo caso è: prima il backup dati/applicazioni, e poi se serve davvero, il reset totale del dispositivo.

Cari bloggers, anche per oggi ho contribuito a rendere il mondo(informatico) un posto migliore(si spera...), pertanto auguro a tutti voi buone feste e un buon inizio anno per il 2013, visto che la fine del mondo è stata rimandata a data da destinarsi a causa della crisi economica... ;-)))

Auguri a tutti :-)

Il comportamento mnemonico degli Hacker (parte 1)

Post n°70 pubblicato il **14 Gennaio 2013** da exodus1984

Carissimi bloggers, oggi come inizio del nuovo anno, vorrei proporre una analisi strutturale dedicata appunto alla mente aperta e avanzata dei soggetti informatici meglio conosciuti e definiti come "Hacker".

Avevo preparato altri nuovi articoli riguardanti l'hardware, ma alcuni amici volevano conoscere le caratteristiche particolari che definiscono appunto l'apprendimento, e la gestione del patrimonio intellettivo proprio di ogni hacker conosciuto su questo pianeta. :-)

Quindi per poterli accontentare, ho dovuto mettere da parte i post che avevo preparato, e scriverne alcuni nuovi, dedicati proprio a questo particolare argomento.

Premetto che questi articoli servono solo a definire i soggetti presi in considerazione, e non a catalogare un hacker diverso da un'altro, per cui questi articoli possono non avere un grande interesse per tutti i lettori di questo blog, ma servono solo come chiarimento per le persone che mi hanno chiesto di effettuare questa analisi.

In questi semplici articoli, cercheremo di definire in modo chiaro e comprensibile per tutti, come funziona davvero la mente di un hacker, senza pretendere però di ottenere la certezza assoluta dovuta alle diverse tipologie di hacker presenti in ogni parte del mondo.

Il concetto, unico per tutti, ma diverso da caso a caso, ci porterà a comprendere i meccanismi della memoria operativa insita in ogni tipo di hacker operativo sulla rete.

Detto questo, iniziamo ad analizzare lo strumento unico per ogni hacker, ovvero il funzionamento della memoria e come viene sfruttata da ogni singolo individuo informatico del pianeta.

In questo primo articolo, cercheremo di capire un semplice meccanismo sfruttato da tutti gli hacker della rete, ovvero le associazioni di idee estremamente ampie e dedicate al particolare ambito ricercato dal soggetto nella rete internet.

Come tutte la facoltà psichiche, è noto che la memoria può andare oltre i limiti imposti dalle normali ricerche in questo particolare campo, è un caso comune che proprio nel sonno, naturale o indotto, si possano risolvere problemi che apparentemente nella realtà e in un particolare momento, non si possano risolvere.

Queste tecniche, si applicano comunemente ad interrogatori con lo scopo di trovare la verità, in cui un servizio d'intelligence può utilizzare farmaci particolari anestetici che eludono la volontà del soggetto, in questi casi, si può notare come il soggetto interessato non si limiti solo a ricordare situazioni particolari, ma nella maggioranza dei casi che ho studiato, il soggetto tende anche a commentare i suoi ricordi, fornendo così un rapporto completo e attendibile sui fatti a lui imputati.

Durante questo periodo in cui la volontà viene annullata dalla narcosi indotta, si può rilevare che il soggetto dice sempre e solo la verità, in quanto mancano i freni inibitori e la volontà specifica di contraddire le proprie affermazioni come invece farebbe nella vita normale, nascondendo e modificando informazioni strategiche che potrebbero costare migliaia di vite umane.

Molti di voi, si staranno chiedendo a che cosa serve parlare del lavoro di una sezione d'intelligence dedicata a questo tipo di lavoro, per cui vi rispondo che il concetto esposto sopra serve a far capire in modo adeguato quanto la mente umana sia allo stesso tempo molto debole e molto forte in base a certi eventi, questi eventi, ci apriranno la strada alla conoscenza di ciò che siamo e di come potremmo essere, ma generalmente, sono imperniati per far capire ai bloggers il vero senso di questi articoli molto particolari che trattano temi poco conosciuti, ma che vorrei spiegare in modo facile e piuttosto conciso per gli amici che hanno fatto questa particolare richiesta.

Come dicevo, per falsare e modificare la realtà, si rende necessaria la volontà stessa per poterla modificare, per cui, non deve mai mancare un vigile controllo di quello che si sta dicendo o facendo in modo da non poter cadere in contraddizione facendosi appunto "scoprire" e mandando a rotoli mesi e mesi di preparazione durante un'operazione segreta, il caso menzionato poco sopra, dimostra appunto che durante una particolare narcosi indotta non si possa affatto mentire, e quindi il soggetto può essere interrogato senza problemi.

Qui mi devo fermare, in quanto questi brevi articoli sono essenzialmente dedicati all'analisi della memoria negli hacker, e non a come vengono svolti certi lavoretti nelle particolari sezioni d'intelligence dei vari paesi del mondo... ;-))

Cari bloggers, concludo questo primo post sperando di avere fatto un po di luce con questa breve introduzione sull'analisi della memoria nella terra degli Hacker, pertanto vi auguro una buona permanenza su internet e ci rileggiamo al prossimo articolo dedicato a questo argomento. :-)

Il comportamento mnemonico degli Hacker (ultima parte)

Post n°71 pubblicato il **15 Gennaio 2013** da exodus1984

Carissimi bloggers, eccoci qui per la seconda parte degli articoli dedicati alla comprensione della capacità di apprendimento degli hacker.

Oggi analizzeremo le cosiddette turbe della memoria, ovvero i disturbi che colpiscono più di ogni altra cosa gli esseri umani e gli animali.

La prassi comune descritta in seguito, è insita da sempre nella natura umana, e questo fa la differenza quando vengono ricercati e scoperti alcuni personaggi definiti "geniali" in rapporto alle persone comuni o definite "normali".

Esaminiamo i principali tipi di turbe comuni della memoria umana:

1) Amnesie

2) Ipermnesia

3) Paramnesia

Queste tre principali turbe della memoria, che vengono poi suddivise in altre categorie più specifiche e relative al soggetto sotto esame, raggruppano quello che potrebbe essere la conoscenza e l'apprendimento di cui un hacker potrebbe avere bisogno, anche se quello che scrivo potrebbe non essere esatto ma serve solo a capire questo argomento, facciamo una breve analisi ristretta per iniziare a capire cosa può succedere alla memoria di un soggetto.

Le amnesie sono in genere disturbi a carattere temporaneo, ma che in casi particolari e documentati, possono essere davvero gravi, possono essere causate da emozioni violente in seguito alle quali si osserva la perdita di ricordi recenti e molte volte di quelli più lontani. Infatti, nessuno può dire che nella propria vita, non abbia mai dimenticato qualcosa...;-)

Le Ipermnesie sono invece di fatto una esaltazione della capacità mnemonica dell'hacker, in cui il soggetto sotto studio, ricorda ogni minimo particolare di un'operazione informatica magari eseguita diversi anni prima, in cui una persona definita "comune", non potrebbe in realtà farlo allo stesso modo.

Questo stato particolare della memoria, definito impropriamente come "memoria fotografica temporale", non risulterebbe del tutto adeguato, in quanto il soggetto vede effettivamente l'azione dei propri ricordi come un film, potendosi soffermare e descrivere qualsiasi particolare gli venga richiesto, e riportando particolari elementi che gli fanno rivedere i suoi ricordi in "altissima definizione", la grande capacità di sintesi e di giudizio nei particolari riferiti, fa di questo atteggiamento mnemonico la base della genialità hacker, molti però convengono che l'ipermnesia possa essere un sintomo precoce di future malattie mentali, ma dovete capire che a tutti gli effetti, un hacker geniale non è una persona comune come tutte le altre, lo è solo in apparenza per il resto della società che vorrebbe osservarlo... :-)

Infine, le Paramnesie sono i disturbi di chi ha la sensazione di essere già stato in alcuni luoghi e di avere già visto certe cose, anche se le vedono di fatto per la prima volta, alcune persone riescono a descrivere il luogo anche prima di poterci andare fisicamente, ma qui entriamo in un argomento un po diverso dalla nostra semplice analisi, per cui mi limiterò solo alle spiegazioni utili e comprensibili per coloro che hanno richiesto queste semplici valutazioni senza però entrare nello specifico che per il nostro articolo, non servirebbe.

Passiamo ora ad esaminare la funzione mnemonica, questa funzione è strutturata in tre stadi ben definiti in cui il soggetto hacker può registrare, conservare e ripresentare il ricordo per risolvere il problema preposto.

1) l'hacker registra il ricordo, in questa fase, la memoria raccoglie di fatto le esperienze del soggetto e le relative intenzioni.

2) l'hacker conserva il ricordo, in questa fase, la memoria fotografica del soggetto archivia la conoscenza e la tiene sempre pronta e disponibile.

3) l'hacker recupera il ricordo partendo dalla situazione reale e cercando di trovarvi una soluzione valida.

Possiamo pensare alla mente di un hacker come ad un immenso database in cui i ricordi e le esperienze fatte, sono "trattenute" in un archivio sospeso tra lo spazio e il tempo, ma accessibile in qualunque momento dal soggetto, che usando la propria volontà, dirige il puntatore al file che gli interessa in un dato momento, rivedendo gli eventi passati come una nuova realtà personale e naturalmente in alta definizione, trovando le diverse soluzioni ai problemi posti nella realtà. :-)

Cari bloggers, con questo articolo, concludo la richiesta che mi è stata sottoposta, spero di essere stato abbastanza chiaro nell'esporre questa semplice analisi della capacità mnemonica degli hacker, augurandovi una buona permanenza in rete, ci rileggeremo presto con nuovi post dedicati.

:-)

Sistemi Operativi Android: le tastiere wireless

Post n°72 pubblicato il **17 Gennaio 2013** da exodus1984

Carissimi bloggers, oggi parleremo di come poter usare una tastiera wireless con il dispositivo Android MK808.

Il dispositivo che è stato testato sui mini pc Android, è la tastiera con touchpad incorporato della Logitech, il modello è il K400r.

Dalle caratteristiche tecniche del Logitech Unifying Receiver fornito in dotazione con questo dispositivo, si può connettere fino a 6 dispositivi(45 è il pairing massimo consentito con un unico ricevitore).

Il software della tastiera può essere scaricato dal sito, per cui, iniziamo a fornire il link per il download del software dal sito del produttore:

http://www.logitech.com/it-it/support/6254?section=downloads&crid=583

Il programma per la gestione del sistema Unifying è disponibile per tutti i sistemi Windows e Mac, ma non ho trovato disponibilità per i sistemi operativi GNU/Linux e Android... :-(

In ogni caso, il suo funzionamento risulta immediato anche sui dispositivi Android che ci interessano, ovvero MK808 Cortex A9, e i GNU/Linux testati con kernel 2.6.32-5-amd64 non ricompilato(installazione base standard).

La manipolazione di questa tastiera, risulta davvero buona, considerando che deve essere usata "al volo" e come dispositivo per la gestione principale dei mini pc connessi al vostro televisore, tutto il sistema appare ben configurato per le principali esigenze dell'utente finale, anche la giocabilità risulta molto veloce, considerando che non si può usare un altro dispositivo. :-)

La suddetta tastiera, è risultata molto utile per le navigazioni internet "veloci", ovvero quando si vuole entrare in rete senza accendere uno dei pc della propria postazione, l'unica cosa da fare è accendere il televisore, settarlo sulla porta HDMI, accendere la tastiera e usare l'internet wifi.

Le due batterie da 1,5 Vcc alcaline fornite con la confezione, hanno una durata stimata di circa un anno, e il dispositivo può contenere al suo interno anche il ricevitore qualora dovessimo trasportare la tastiera su altre macchine o postazioni diverse.

I pulsanti sono disposti in modo ottimale, sia per scrivere testi con il LibreOffice che per manipolare la sospensione del proprio portatile o del dispositivo Android.

In effetti, questa tastiera risulta l'ideale per poter lavorare in modo adeguato se dovete connettere la vostra LinuxBox al televisore da 32 pollici, personalmente, ho trovato in vendita questo dispositivo e ho voluto provarlo, posso dire che però esistono anche moltissimi altri tipi di tastiere e mouse che potevo prendere, ma alla fine ho scelto questa per il prezzo(38 euro) in confronto ad altre disponibili ma molto più piccole di questa, tanto per intenderci: con i tasti piccoli come quelli di un cellulare, e che costavano 50++ euro... ;-))

Per il lavoro che deve svolgere, il prezzo è un pochino alto, ma dopo tutto, è costruita per questo particolare uso, e concordo benissimo che su internet avrei potuto trovare di meglio e anche a prezzi più bassi, ma alla fine, sono comunque rimasto soddisfatto di questo dispositivo. :-)

Le mie intenzioni principali erano di trovare un dispositivo adatto soprattutto a scrivere testi elettronici e che avesse un minimo ingombro, per cui devo dire che questa tastiera è l'ideale e molto confortevole se

dovete scrivere molto, ma se avete altre possibilità, cercate e valutate di persona quello che potrebbe servirvi davvero per il vostro lavoro.

Cari bloggers, anche per oggi abbiamo terminato questa breve verifica tecnica per un hardware che forse può risultare utile a molti di voi. :-)

Come sempre, una buona navigazione e un buon proseguimento a tutti voi su internet :-)

Racconti elettronici: P.V.D.I.O.G.

Post n°73 pubblicato il **21 Gennaio 2013** da exodus1984
Carissimi bloggers, oggi sto riflettendo su alcune cose che riguardano l'epoca in cui viviamo, ma più che altro cerco di creare qualcosa che possa far riflettere anche i navigatori occasionali di questo piccolo blog.

Per questo motivo oggi, vi voglio regalare un capitolo importante scritto tempo fa per l'inizio di un nuovo libro elettronico al quale sto lavorando quando il tempo e il lavoro me lo permettono.
Questo racconto di fantapolitica, agli inizi era stato scritto e modificato più volte, in base alle informazioni raccolte nel tempo per dare agli utenti un qualche cosa di verosimile alla realtà.
Infatti non ho ancora terminato la sua scrittura, proprio perché il mio tempo è limitato, però mi piace condividere con i bloggers di Libero quello che faccio, anche perché sul blog si possono avere dei commenti che potrebbero migliorare le mie semplici capacità personali in questo campo, infatti non sono uno scrittore professionista, e questo, fa di me una persona normale, anche se nella vita, scrivo e leggo molto.... :-)

P.V.D.I.O.G. (...titolo sperimentale spippolato...) ;-))

Licenza CCPL BY-NC-ND ver. 3 - P.V.D.I.O.G. 2012 versione 1.0.1

La Morte del Mondo

Gli uomini guardarono morire il proprio mondo, strangolato dalle corporazioni finanziarie che esigevano sempre più tributi.
Le tasse rendevano più poveri gli uomini, e non garantivano per nulla i servizi sponsorizzati dal Governo per mantenere sotto controllo la popolazione.
Nel mondo del ventunesimo secolo, la morte per povertà era all'ordine del giorno, l'Italia di quel tempo, era diventata un covo di ladri e assassini che per garantirsi il potere assoluto sui pochi cittadini onesti rimasti, eliminava ogni tipo di prova per eludere i tentativi di insurrezione del popolo stremato dalle tasse e dalla avidità dei politici.
L'Italia, non era l'unico paese europeo ad essere stato distrutto dalla avidità di pochi ma potenti uomini appartenenti ad una corporazione finanziaria segreta che operava in ogni parte del pianeta.

Come si era potuti arrivare a tutto questo? Il lavoro, la vita e la proprietà di ogni singolo individuo sulla faccia della Terra, non aveva
più alcun valore, la ribellione alla corporazione, era punita con la morte, per cui, nessuno ormai osava opporsi a questi uomini avidi che oltre che i loro soldi, si sarebbero presi anche le loro vite.
La recessione economica globale aveva distrutto ogni forma di impresa, il valore del lavoro era praticamente nullo.
Questo era il tempo della miseria umana più totale, mentre pochi godevano il frutto del sudore della fronte di altri, il resto del mondo stava a guardare in silenzio, per paura di perdere anche le poche essenziali cose che gli erano rimaste.
Le rivolte di protesta del 2013, avevano distrutto tutto ciò che ancora era rimasto della società europea, ma nessuno si sarebbe più preoccupato di questo, perché la guerra civile era appena iniziata.

Fu allora che un manipolo di uomini raccolse questa grande sfida, per poter
tornare ad essere liberi e non oppressi dalle corporazioni finanziarie che avevano distrutto le loro vite.
In un periodo storico molto travagliato come questo, ci fu chi credette ancora nella speranza e nella rinascita della nostra società, e questo ci rese di nuovo liberi.
Gli antichi membri del primo consiglio internazionale libero, dopo la fine della guerra civile europea si accordarono per scrivere la carta dei diritti dei liberi cittadini, e questo portò ad una nuova nazione e ad un nuovo popolo unito per sempre da una sola parola: Libertà.

P.V.D.I.O.G.

Licenza CCPL BY-NC-ND ver. 3 - P.V.D.I.O.G. 2012 versione 1.0.1

Cari bloggers, anche per oggi è tutto, augurandovi una buona navigazione su internet, ci rileggeremo ai prossimi post. :-)

Sistemi Operativi Android: rootiamo il sistema del dispositivo MK808.

Post n°74 pubblicato il **22 Gennaio 2013** da exodus1984
Carissimi bloggers, oggi ci occuperemo come al solito di spippolamenti informatici, a questo proposito, parleremo di come ottenere un dispositivo MK808 Android rootato per tutte le nostre prove tecniche. :-)

Iniziamo con le consuete procedure di partenza, preparate il vostro televisore da 32 pollici acceso, settate il telecomando del TiVu' sulla porta in ingresso HDMI dedicata al vostro dispositivo Android e connettete la vostra rete interna Wi-Fi per raggiungere internet.

Prima di ogni altra cosa, bisognerà "rootare" il dispositivo Android con una app che avrete scaricato ed installato in precedenza.
Per le prove di rito, ho usato l'app SuperSu v. 0.99, disponibile nel play store di Google, questa app, permette una perfetta configurazione del dispositivo, e contiene diverse opzioni sia per settare meglio il proprio sistema Android, sia per effettuare la pulizia completa per l'UNRoot del sistema e riportare alla normalità il tutto nel caso qualche versione strana di Android non digerisca bene questi spippolamenti particolari... ;-))

SuperSu dispone di tre schede ben definite in cui si può fare quasi tutto sul dispositivo rootato, ma non proprio tutto, perché alcune funzioni, sono proprie della versione SuperSuPro a pagamento, ma per i nostri test, ci basta l'app gratuita per il momento, in quanto nel periodo di test, possiamo decidere se passare o no alla versione a pagamento con la quale non avremo limiti di operatività sul sistema Android. :-))
Le tre schede di SuperSu, sono rispettivamente: APPS, LOG e IMPOSTAZIONI, dove appunto faremo le nostre scelte per la configurazione che vogliamo avere.
Nella scheda APPS, avremo a disposizione tutte le applicazioni che richiedono un dispositivo Android rootato, e quindi ci apparirà come prima app installata il coltellino svizzero dei sistemi operativi, ovvero il leggendario tool di strumenti applicativi compatti con il quale ci potremo divertire davvero molto: chi non conosce BusyBox? ;-))
Naturalmente, nei test che ho eseguito, BusyBox è stato installato dopo il root del sistema Android, in quanto esiste una sua procedura che ora andremo a vedere insieme.

A questo punto se tutto è andato come richiesto, avete il sistema Android rootato per iniziare tutti i vostri test tecnici.
Adesso è giunto il momento di scaricare e installare il tool BusyBox che ci permetterà di usare in modo aperto e completo il nostro dispositivo Android.
Sempre dal Play Store di Google, effettuate una ricerca applicativa per BusyBox, la versione è la 1.20.2, completa di interfaccia per l'installazione sul sistema Android.
Al primo avvio l'app BusyBox controlla l'installazione, e dopo aver valutato il sistema, richiede all'utente di premere un tasto freccia: tasto freccia basso, viene selezionata in colore giallo l'installazione, dopo questo primo passaggio, dovete cliccare sul pulsante in basso "INSTALL", le altre due voci rimanenti per la scelta dell'utente sono: "UNINSTALL" e "RESTORE".

BusyBox installa il suo sistema nella directory standard /system/bin/ , però se volete giocare ai tamarri di rete, consiglio a tutti di provare altre directory dove potrete fare tutto quello che volete al vostro povero dispositivo Android... ;-)))

Ora per completare il tutto, preleviamo dallo Store una simpatica app che ci sarà davvero molto utile, in modo particolare a chi come me è abituato ad usare un terminale di puro testo per girare tutto il sistema Android... ;-))

Ricercate sullo Store questa app: Android Terminal Emulator
potete controllare il Wiki link se desiderate avere ulteriori dettagli su questa app al seguente indirizzo:

http://github.com/jackpal/Android-Terminal-Emulator/wiki

Android Terminal Emulator è un progetto Open Source, la versione è la 1.0.50, per cui ogni informazione che impariamo su questo e altri progetti, ci sarà utile per le nostre prove.
Nella configurazione di A.T.E. dovete ricordarvi di settare l'opzione "MOSTRA/NASCONDI TASTIERA", questa opzione, disabilita la tastiera virtuale che appare sullo schermo ogni volta che digitiamo qualche cosa, in pratica, vi serve per avere il terminale libero e perciò anche più grande, senza avere appunto lo stress della tastiera virtuale sempre visibile... ;-)))

Dunque, concludendo questo breve articolo dedicato ai dispositivi MK808, adesso che abbiamo installato e configurato queste tre app Android, ci possiamo rilassare un po prima di passare al definitivo assalto del dispositivo Android... ;-)))

Cari bloggers, anche per oggi è tutto, come sempre vi auguro una buona navigazione e una buona permanenza su internet. :-))

Breve guida per la prevenzione delle truffe: le carte di credito e la sicurezza.

Post n°75 pubblicato il **03 Febbraio 2013** da exodus1984
Carissimi bloggers, oggi parliamo di un argomento che ci tocca tutti quanti, almeno per quelli di noi che usano le carte di credito e i vari bancomat.

Questi post, sono mirati a far comprendere alle persone il corretto approccio da tenere nei vari luoghi dove usiamo il nostro strumento di pagamento personale, ma hanno anche un fine di apprendimento delle tecniche di base usate dai truffatori per impadronirsi del conto personale della vittima prescelta in modo che gli utenti possano capire come funzionano queste truffe e quindi reagire mettendo in sicurezza per quanto possibile, i propri soldi.

Oggi, inizieremo a capire quali sono i metodi più semplici usati dai truffatori per impadronirsi dei dati contenuti nelle vostre carte di credito e nei vostri bancomat.

Molto tempo fa, in una galassia lontana lontana... ;-)))
Ebbene, molto tempo fa, venivano usate tecniche diverse per arrivare allo stesso obiettivo, ovvero prelevare soldi da un conto non proprietario e usarli per scopi non proprio didattici... :-)))

Ok, fin'ora ho scherzato un po, ma quello che andremo a vedere adesso, forse vi potrà convincere a prestare un po più di attenzione quando maneggiate tutte le vostre carte di credito e i vostri bancomat.

Esistono migliaia di tecniche con cui un ingegnere sociale può ottenere informazioni utili sulle vostre carte di credito, ma questo non è ancora tutto quello che dovrete imparare per potervi difendere, infatti la truffa è sempre dietro l'angolo, e non potrete mai sapere in anticipo come e quando verrete truffati, in effetti, sarebbe davvero fantastico saperlo in anticipo, ed è per questo che ho deciso di scrivere un post di questa portata.

Parlando di bancomat, vi posso dire che le tecniche usate sono davvero ai limiti dell'incredibile, per esempio: un truffatore che non usi hardware per catturare i dati delle bande magnetiche inserito come copertura nei vari sportelli adibiti al prelevamento di contanti, può usare altri sistemi, in particolare macchine fotografiche con teleobiettivi, in questo caso come ci possiamo difendere?
La prima cosa da fare, è quella di controllare lo sportello automatico e verificare che non ci siano "gabole" strane appiccicate nei punti di inserimento delle tessere, quindi coprire la visuale quando digitate il vostro codice e controllare che qualche "strano" esemplare umano, non stia sbirciando alle vostre spalle... :-))

Ma voi penserete che queste sono cose del tutto normali vero? :-)
Allora leggete qui:

Durante un test di sicurezza che ho condotto su un centinaio di persone tutte prese a pagare con il proprio bancomat o la carta di credito alle casse di un supermercato, ebbene, tutte queste persone, non hanno posto nessuna barriera fisica tra la digitazione del loro codice personale e il numero di carta di credito presente sulle loro tessere personali dallo sguardo indiscreto di una persona comune e innocente come me... ;-)))

Questo post è stato scritto proprio per questo motivo, la gente non tiene conto che quando paga con la propria carta, non siano al sicuro da elementi "strani" che sbirciano il codice digitato e il numero della carta con il solo scopo di ottenere il denaro del loro conto e di utilizzare le loro carte di credito in modo truffaldino.

Come possiamo difenderci da questi assalti "invisibili" agli occhi delle persone normali?
Ci possiamo difendere conoscendo le tecniche usate, e rispondendo di conseguenza con una difesa "attiva".

attacco 1:
una persona in fila alla cassa dietro a voi armeggia e finge di giocare con il cellulare.

difesa 1:
quando prelevate la vostra carta, assicuratevi di coprire il numero e la tastiera quando digitate il vostro codice segreto.

attacco 2:
una persona o due, vi affiancano nella fila per pagare in cassa, sembrano persone comuni, ma attendono di vedere la vostra carta.

difesa 2:
pretendete sempre una certa distanza dalle persone che vi affiancano, perché non sempre sono andate al supermercato per comprare qualcosa...e molto probabilmente si compreranno qualcosa con i vostri soldi... :-)

Ecco perché bisogna essere preparati, nel secondo attacco, non esistono tecnologie avanzate, ma la complicità di due o più persone che entrano ed escono dal supermercato con il solo scopo di catturare quanti più numeri e carte possibili... :-)

Facciamo un banale esempio, il truffatore cattura un numero di carta di credito, la prima cosa che potrebbe fare, sarà quella di accertarsi che il numero catturato possa rispondere alle sue esigenze, ovvero capire a quale circuito appartiene, a quale banca fa riferimento, quale sia il numero di conto corrente dell'intestatario e procedere quindi con un attacco mirato.

Osservate qui di seguito, uno tra i più usati algoritmi di validazione:

Numero di carta di credito di esempio:

```
 p d p d p d p d p d p d p d p d
 2 0 2 0 2 0 2 0 2 0 2 0 2 0 2 0
```

1) da destra a sinistra moltiplicare per 2 le cifre pari:

```
 2 0 2 0 2 0 2 0 2 0 2 0 2 0 2 0
 p d p d p d p d p d p d p d p d
```

2) se le moltiplicazioni portano a numeri di 2 cifre, bisogna sommarli
per ottenerne uno solo.

```
 p d p d p d p d p d p d p d p d
 2 0 2 0 2 0 2 0 2 0 2 0 2 0 2 0
 p x 2 = ?
 4 0 4 0 4 0 4 0 4 0 4 0 4 0 4 0
```

3) ora si sommano le cifre ottenute dalle moltiplicazioni con i numeri
dispari per ottenere la "cifra di Lhun".

```
 p d p d p d p d p d p d p d p d
 2 0 2 0 2 0 2 0 2 0 2 0 2 0 2 0
 p x 2 = ?
 4 0 4 0 4 0 4 0 4 0 4 0 4 0 4 0
 4 0 4 0 4 0 4 0 4 0 4 0 4 0 4 0
 4+4+4+4+4+4+4+4=32      p+d
 32 = cifra di Lhun
 32---> 32 se la cifra divisa per 10 non è intera, il numero non è valido
 32/10 = 3.2 numero non intero, quindi non valido
```

32 diviso 10 da 3.2 ovvero 3 con il resto di 2
in questo caso la cifra di Lhun sarà 8 (10-2)

4) Analizziamo ora un esempio di codice valido:

p d p d p d p d p d p d p d p d
2 0 2 0 2 0 2 0 2 0 2 0 2 4 2 0
p x 2 = ?
4 0 4 0 4 0 4 0 4 0 4 0 4 8 4 0
4 0 4 0 4 0 4 0 4 0 4 0 4 8 4 0
4+8+4+4+4+4+4+4+4=40 p+d
40/10=4 numero intero senza resto, risultato valido

Da questo banale esempio, potete capire perché dovete coprire sempre il vostro numero di carta da occhi indiscreti, perché è proprio il vostro numero che rivela ai truffatori tutto quello che vi appartiene.... :-)

Su internet esistono i cosiddetti "Carders" che si occupano proprio di scambiare numeri validi di carte di ogni tipo in cambio di soldi.
Le truffe tecnologiche più avanzate, vengono portate a termine da gruppi scelti e preparati dal crimine organizzato, che usa questo modo per racimolare denaro da inserire in altre attività, ci sono poi i cosiddetti
gruppi di "sopravvivenza" che usano queste tecniche non per accumulare denaro ma proprio per sopravvivere nel vero senso della parola... :-)
Infine, chi lo fa per divertimento, per ragioni di sicurezza o per svariati altri motivi, ma non per denaro... :-)

Detto questo, ne approfitto per ringraziare alcuni amici di vecchia data a cui avevo promesso la verità, e ciò che viene promesso, deve essere anche mantenuto.
Per cui, pensate bene a questo post la prossima volta che dovrete pagare la spesa al supermercato con la vostra carta di credito preferita... ;-)

Cari bloggers, anche per oggi è tutto, ricordate che la conoscenza è potere, ma che questo potere deve essere usato per il bene della comunità e non contro di essa.
Con questo, vi auguro una buona permanenza e una buona navigazione su internet. :-)

Riflessioni personali e notizie locali

Post n°76 pubblicato il **24 Febbraio 2013** da exodus1984
Carissimi bloggers, oggi vorrei parlare di un argomento che sta facendo il giro del mondo, ovvero la tragedia che ha colpito un atleta che tutti abbiamo visto qui a Gemona.
Nella giornata di ieri, ho notato un gran movimento di giornalisti che facevano molte domande alla gente, e naturalmente poi ho scoperto anche il perchè... :-)
Il sindaco di Gemona, vorrebbe andare a testimoniare la solidarietà della nostra città a questo atleta che per un periodo ha soggiornato in uno dei nostri hotel, ma potrebbe trattarsi solo di un'iniziativa personale, non legata al caso internazionale che ha coinvolto l'atleta, ma essendoci un processo in corso, la cosa ha scatenato alcune polemiche con alcuni rappresentanti del locale consiglio comunale perchè giudicato un atteggiamento forse troppo di parte verso l'atleta, questo è quanto ho sentito dire qui in giro.
A parte questo, io ritengo che non sia il caso di fare ulteriori polemiche anche per rispetto verso questo atleta colpito da una tragedia di questa portata.

Per chi si stia chiedendo il perchè di tutti questi giornalisti in città, la cosa è presto chiarita, forse ci potrà essere un altro collegamento qui da Gemona già da martedì pomeriggio con la trasmissione televisiva "La vita in diretta".

Cari bloggers, anche per oggi è tutto, ci rileggiamo alle prossime e come sempre vi auguro una buona navigazione e un buon divertimento su internet.

Guarigioni miracolose: le truffe "elettroniche" globali tra la fine del 1800 e l'inizio del 1900

Post n°77 pubblicato il **25 Febbraio 2013** da exodus1984
Carissimi bloggers, oggi ho fatto una ricerca per uno strumento giudicato "miracoloso" nel lontano 1904... :-))

Andiamo quindi ad aprire il portale del tempo e cominciamo ad indagare su alcune truffe spettacolari del nostro antico modo di vedere la medicina, e le applicazioni "mediche" create con l'avvento dell'elettricità... :-)))

Le bufale si trovavano anche a quei tempi, non solo nella nostra epoca...;-)
Dunque, dicevo che ho fatto questa ricerca perché in possesso di antichi documenti firmati dal Dr. Mac Laughlin.
La sede per l'Italia era a Milano, in via Ugo Foscolo 3,

In questo documento storico battuto a macchina e firmato con penna a calamaio nel lontano 1904, si esaltano le capacità di guarigione tramite la corrente elettrica di molte malattie sessuali, molto comuni all'epoca.
Questa cintura miracolosa, doveva curare l'astenia sessuale come prima cosa, ma dal documento in mio possesso, si può notare che praticamente tutto il corpo poteva trarne beneficio... ;-)))
Questa cintura era composta da una catena di pile ai capi delle quali erano posizionati degli elettrodi sul dorso, potete solo immaginare a cosa potesse servire lo "strano" cilindro metallico e dove doveva essere posizionato per ridare vigore all'uomo... :-)))

In questi documenti storici originali, si esaltava oltre misura la capacità di guarigione, che a tutti gli effetti, portò a diverse "guarigioni", dovute essenzialmente all'effetto "placebo" che la pubblicità dell'epoca fece per promuovere questo strano e quanto inutile strumento "medico"...:-)))

Per chi decideva di "guarire", il costo era di Lire 175, che comprendeva l'apparecchio descritto e i consigli per l'uso, naturalmente, il costo di questa macchina miracolosa, doveva essere inviato prima alla società che gestiva le vendite, perché il contrassegno non era previsto...:-))

La cosiddetta "guarigione", avveniva in circa dieci giorni, usando la cintura prevalentemente di notte, e se il paziente era considerato grave, il periodo di "cura" si aggirava addirittura ad un mese intero...:-)))

Il paziente che tentava questa cura, doveva riempire un questionario e spedirlo a degli "esperti" che valutavano il singolo caso, aggiungendo anche una lettera accompagnatoria alla cintura elettrica, nella quale il soggetto riceveva numerosi consigli da esperti di "fama internazionale", mirati più che altro ad ottenere una "suggestione medicale" che ha guarito come detto in precedenza, usando l'effetto placebo ma non con la reale cintura miracolosa... :-)))

Continuando a leggere queste antiche pagine, mi viene da ridere pensando a quanti "polli" ci sono cascati, in realtà, la cintura funzionava a livello elettrico, la debole corrente emessa era niente in confronto alla tensione raggiunta, immaginate 35-40 volt applicati alle parti intime in modo diretto per almeno 8 ore...:-)))
Sulla rete sono disponibili numerosi schemi elettrici per la costruzione di queste macchine, per chi volesse cimentarsi nell'impresa...:-))

Ritornando ai suddetti documenti, si potevano trovare sedi ovunque, sia in Europa che in America, Canada e Australia, se penso a quante persone
che ci sono cascate anche per via dell'ignoranza e dell'analfabetismo molto comune a quel tempo, mi chiedo se nella nostra epoca, considerata tecnologicamente avanzata, non si possa fare di meglio...;-)))

I numeri dei cellulari??? :-))
Le carte di credito??? :-))
I Bancomat??? :-))

Ok, ho scherzato un po per sdrammatizzare la situazione, ma in Italia
ne furono vendute moltissime di queste cinture all'epoca, si potevano trovare persone indebitate fino al collo per potersi pagare questa "cura miracolosa", ma questa è solo un'altra storia di fame e povertà del nostro antico paese, il documento in mio possesso, originale e ben conservato, scritto in lingua italiana

dell'epoca molto particolare, mostra diverse sfumature nel raccontare le proprietà dell'elettricità a cavallo tra il diciannovesimo e l'inizio del ventesimo secolo.

Le truffe continueranno sempre, in ogni epoca, in ogni tempo e in ogni luogo, essere preparati per affrontarle, è un dovere di ogni essere umano, per cui, cari bloggers, non seguite questi esempi... :-))

Anche per oggi è tutto, di nuovo a tutti voi, una buona navigazione e una buona permanenza in rete.

Sistemi Operativi: i RootKit sui moderni sistemi Windows.

Post n°78 pubblicato il **09 Marzo 2013** da exodus1984
Carissimi bloggers, oggi vorrei portare la vostra attenzione su un fenomeno antico del mondo informatico, ovvero l'uso sempre più frequente di sistemi rootkit installati sui moderni sistemi Windows.

In origine, il termine informatico "rootkit" fu coniato sui sistemi operativi Unix, sistemi peraltro appartenenti a grandi aziende e sistemi governativi e militari, in parole povere, le reti che potevano essere controllate per prelevare informazioni strategiche e industriali.

Forse pochi di voi ricorderanno uno dei primi Eurocrypt, tenuto proprio qui a Udine nell'ormai lontano 1983, in cui i partecipanti italiani si potevano contare sulle dita di una sola mano, erano presenti matematici, operatori di intelligence, programmatori e diverse spie industriali interessate alla protezione crittografica delle informazioni sensibili. :-)

Molti di voi si staranno chiedendo a che cosa serva ricordare una antica conferenza sulla crittografia con i rootkit attuali, per cui fate molta attenzione, capirete la risposta più avanti... :-)

Nel 1984, l'Italia brulicava di spie, e la tecnologia italiana dell'epoca, era considerata la più appetibile per gli agenti sovietici formati nella scuola di Piazza Dzerzhinsky, ovvero la sede del KGB a Mosca.
Il metodo era semplice, tenere d'occhio il soggetto interessato (programmatori, matematici, etc.etc...), quindi il soggetto veniva invitato a varie feste organizzate allo scopo di "convertire" la persona prescelta alla grandezza e alla bontà della causa sovietica, per poi ricattarla con lo scopo primario di ottenere informazioni industriali e segreti militari come i piani del Tornado, frutto della migliore tecnologia tedesca, italiana, e britannica. :-)
In Italia, il KGB era particolarmente interessato ai processi industriali dell'epoca, tra cui i procedimenti segreti sulla composizione di leghe speciali tecnologicamente avanzate prodotte dal nostro paese, questo per il ramo industriale, mentre per il settore militare, veniva considerato il carro armato Leopard, per il suo alto contenuto tecnologico, e le fregate di classe "Lupo" e "Maestrale" per lo studio dei sistemi di puntamento e dei sistemi radar avanzati.
Il Friuli, era una zona di passaggio per tutte le spie che entravano e uscivano dall'Italia, e la genialità italiana era considerata all'epoca una delle maggiori fonti di sviluppo tecnologico e militare per i paesi dell'est europeo.

Ma torniamo all'argomento del post in questione, perché vi ho raccontato tutto questo?
Il motivo è semplice ed intuitivo, le informazioni industriali, sono sempre appetibili non solo per i servizi di intelligence, ma anche per semplici utenti intenzionati a rivenderle al miglior offerente.

Da questo, concludiamo che i rootkit sono strumenti utilissimi per questi scopi, per esempio, se vogliamo controllare una persona, dovremmo disporre di un rootkit preparato per il suo sistema, a questo scopo, possiamo scegliere tra due differenti tipi di rootkit, il rootkit in modalità amministrativa oppure il rootkit in modalità utente.

Molti di voi potrebbero prediligere i rootkit a livello amministrativo, che danno una maggiore autonomia sul sistema sotto controllo, ma il rootkit in modalità utente, risulta utilissimo quando si devono prendere informazioni esclusive da un determinato account, senza per questo rischiare di essere scoperti a livello amministrativo, e comunque, senza compromettere l'intero sistema sotto controllo.

Ho scritto questo breve post sui sistemi complessi di rootkit per Windows al solo scopo di informare gli utenti di questo sistema operativo di quanto possano essere vulnerabili e preziose le informazioni contenute nei loro account, infatti negli ultimi tempi, ho potuto valutare che i singoli virus progettati per questi sistemi, tendono a diminuire in favore di rootkit preparati appositamente per il controllo degli utenti e delle loro informazioni personali.

Analizziamo dunque il funzionamento di base di un banale rootkit per sistemi Windows:

Il rootkit si compone di due elementi basilari per il suo funzionamento, il primo elemento è detto "iniettore", e serve per indurre il sistema operativo sotto attacco ad eseguire il codice, può essere un messaggio di posta elettronica oppure un utente che usa l'account amministrativo di Windows per navigare su internet.
Il secondo elemento utile di un rootkit, è il cosiddetto payload, ovvero il carico utile, che è quello che a tutti gli effetti, porterà a termine il controllo dell'utente o dell'intero sistema operativo.

Il rootkit, si aggancia al kernel di Windows mascherandosi da driver di sistema oppure se in modalità utente, come un semplice programma che l'utente stesso usa con più frequenza rispetto ad altri programmi. :-)

Dopo avere modificato il comportamento del kernel di Windows tramite driver di dispositivo che controllano le chiamate standard di sistema, il rootkit esegue una cifratura forte sui suoi contenuti e sui dati catturati a livello utente e amministrativo, in modo che si possa ottenere un buon livello di sicurezza per le informazioni trafugate all'insaputa del proprietario del computer.

Le banali tecniche fin qui descritte, non rendono giustizia però ai rootkit progettati in modo esclusivo per il controllo specifico di una determinata rete industriale o governativa, nei moderni rootkit per sistemi Windows, vengono occultati gli utenti di rete, viene eliminato ogni riferimento reale nella lista dei processi attivi di sistema, consentendo al rootkit di risultare completamente invisibile alle scansioni di antivirus e degli IDS(intrusion detection system), infine, la personalizzazione di un rootkit, permette di essere totalmente invisibili sul sistema posto sotto controllo, e quando il sistema risulta compromesso ad un livello così profondo, non resta altro che effettuare una nuova re installazione del sistema operativo da backup certificati.

Per cui, tutti gli utenti di Windows che usano i loro computer con utente amministrativo sono a rischio, ma questo non toglie che anche la creazione di un utente senza privilegi possa portare se non al controllo completo del sistema, anche solo al controllo del semplice utente, in fondo si tratta sempre di ottenere un unico dato importante: l'informazione.

Sui rootkit per sistemi Windows, si potrebbe scrivere una intera enciclopedia, visto che la sicurezza finale di questi sistemi viene affidata solamente all'utente finale, che non essendo preparato nel 99% dei casi, è il primo veicolo di infezione che permette ad un intruso di rete di controllare il suo sistema.

Naturalmente, non tutti gli utenti che comprano un PC sono alle prime armi, però il resto di loro è un'esca molto appetitosa per hacker che vogliono usare il computer di un'altro per rimanere anonimi, mentre in rete ne combinano di tutti i colori, facendo ricadere la colpa sul computer connesso in rete dal vero proprietario...:-)

Nelle ultime settimane, durante i corsi di formazione e sicurezza informatica che ho tenuto appositamente per spiegare l'evoluzione di questo fenomeno informatico che come dicevo in precedenza, ha radici molto antiche, ma è terribilmente attuale, molti utenti sono rimasti colpiti da questa affermazione che può trovare riscontro presso molti siti web su internet dedicati proprio alla configurazione e all'uso dei rootkit in ambiente Windows.

Proprio durante una recente lezione di sicurezza informatica, ho potuto far vedere agli utenti del corso, un computer portatile compromesso da un rootkit, questo rootkit, impersonava il programma di connessione di una chiavetta internet della Vodafone, in pratica, ogni volta che l'utente tentava di connettersi ad internet usando il programma di connessione, il rootkit memorizzava i dati da inviare alla prossima connessione in modo criptato, ma senza permettere all'utente di connettersi dal portatile con la suddetta internet key...:-))

Quindi, il povero utente non poteva usare la internet key in modo diretto
dal portatile, perché il rootkit aveva già scovato le password amministrative della rete wi-fi aziendale, per cui, quando l'utente lavorava con la rete wireless, poteva accedere ad internet assieme al pirata che ha usato il suo computer portatile come "porta di accesso" alla rete mondiale rimanendo anonimo perché coperto dalla rete aziendale compromessa da un computer Windows gestito male...:-)

Devo dire che questo rootkit era preparato molto bene, ma non tanto bene da poter sfuggire alla mia esperienza diretta sul campo. :-)))
Questo rootkit ha eluso perfettamente il firewall installato sul sistema Windows, usando una tecnica particolare chiamata "portknocking", infine ha aggirato le scansioni dell'antivirus installato, facendo credere all'utente che il sistema fosse in perfette condizioni operative... :-))

Dovendo capire il perché di questo particolare comportamento sul sistema Windows 7 Pro installato su un computer portatile usato per lavoro in una azienda importante della zona, ho subito sospettato l'esistenza di un programma di questo tipo, ma conoscendo bene la particolare architettura di un rootkit, ho dovuto eseguire alcune semplici tecniche per poterlo scovare sul sistema, ma purtroppo, non posso sapere quanto in profondità sia andato per tentare un effettivo recupero del sistema Windows compromesso, e non sono nemmeno certo che i dischi di backup forniti dall'amministratore di rete siano attendibili per poter ripristinare il sistema sul portatile, visto ed appurato che il pirata ha mirato alla rete

e non all'utente singolo... :-(

Facendo il terzo grado all'utente proprietario del pc, ho scoperto il suo modo di lavorare su internet, e constatando gli enormi buchi di sicurezza lasciati liberi da questa persona per la poca esperienza con il computer fornito dall'azienda, ho potuto catturare sia il rootkit che l'account di rete nascosto sul sistema in modalità utente, ma con permessi amministrativi completi e anonimi... :-))

Naturalmente, gli utenti del corso sono rimasti perplessi da un tipo di assalto informatico di questa portata, e benché molti di loro conoscano bene i danni prodotti dai rootkit, non ne avevano mai visto uno all'opera su un sistema e non erano stati capaci di rilevarli, spiegando questo tipo di assalto informatico e facendo vedere le prove fisiche su un sistema reale, tutta la teoria che avevano imparato sui virus e i rootkit ha ceduto il posto ad un reale senso di paura per la perdita dei propri dati informatici archiviati. :-)

Quando ho deciso di pubblicare questo breve articolo, i rootkit scoperti erano circa sei su dieci utenti, quindi ho pensato bene di postare questo articolo anche per informare le persone che usano i loro sistemi Windows pensando che il firewall e il loro antivirus li possano proteggere da tutto questo.

Ricordate che è perfettamente inutile possedere un livello di sicurezza ritenuto "elevato" quando si affida un computer aziendale ad una persona che di fatto sa usare solo le funzioni principali di connessione e condivisione della rete, e oltretutto, le usa male, anche se non per causa sua... :-)
I dipendenti delle aziende dovrebbero sempre adottare i parametri di sicurezza informatica prescritti dall'azienda, cosa che purtroppo, non sempre accade...:-(

Cari bloggers, anche per oggi è tutto, e se potete farlo, siate sempre un pochino paranoici riguardo ai sistemi che vi vengono affidati, perché rischiate seriamente di compromettere non solo la vostra sicurezza informatica personale, ma anche quella di tutti gli altri dipendenti della vostra azienda. :-)

Ultimo saluto.

Post n°79 pubblicato il **23 Marzo 2013** da exodus1984
Questo semplice post è dedicato ad un grande amico con cui ho condiviso la mia preparazione informatica e tecnologica, ci siamo ritrovati tutti quanti oggi per darti l'ultimo saluto.

Tratto dalla musica che ascoltavi sempre:

"Mi farò strada fra 100 miliardi di stelle, la mia anima le attraverserà, e su una di esse vivrà eterna."

La conoscenza che hai cercato qui sulla Terra, ora ti appartiene per l'eternità.
Buon viaggio amico mio, e grazie per tutto quello che ci hai insegnato.

Dai tuoi amici, i "ragazzi di internet".

Sistemi Operativi: C.A.IN.E. 4 (Computer Aided Investigative Environment)

Post n°80 pubblicato il **25 Marzo 2013** da exodus1984
Cari bloggers, oggi voglio parlare della nuova release di C.A.IN.E.

Per scaricare l'iso da masterizzare potete seguire questi link:

http://www.caine-live.net/page5/page5.html

Il primo file Caine4.0.iso è dedicato alla masterizzazione su CD/DVD, mentre il secondo file NBCAINE 4.0 è un iso dedicato ai portatili netbooks, e potete usare i programmi seguenti per crearvi una distro portatile per analizzare i sistemi senza danneggiarli.

Qui di seguito, trovate una breve selezione dei principali programmi usati su Linux e windows per creare key USB bootabili, che vi permettono di portarvi in giro tutti i vostri sistemi operativi per la manutenzione dei PC, portatili e fissi.
Per creare una key usb bootabile da sistemi Windows, andate a questo link e scaricate il programma proposto:

http://rufus.akeo.ie/

Rufus is a small utility that helps format and create bootable USB flash drives, such as USB keys/pendrives, memory sticks, etc.

programma da scaricare ---> Rufus v1.3.2 (442 KB)

Se invece volete un tool davvero tosto, allora dovete provare UNetbootin, potete scaricarlo dal suo sito:

http://unetbootin.sourceforge.net/

i pacchetti sono molteplici per sistemi operativi GNU/Linux, WinXXX e Mac++ ;-)

Potete leggere il sito dedicato alla distribuzione per gli help in linea, se non
vi trovate a vostro agio con questo sistema GNU/Linux molto particolare.

Più avanti cercherò di preparare un post non troppo tecnico per spiegare a tutti coloro che di informatica non se ne intendono, la bellezza di questa distro live.

Cari bloggers, anche per oggi è tutto, buona navigazione a tutti e buon divertimento su internet. :-)

Il Sacro Corano: il progetto Zekr e le applicazioni scaricabili per PC, Tablet e Cellulari

Post n°81 pubblicato il **20 Aprile 2013** da exodus1984
Carissimi bloggers, oggi vorrei presentare alcune applicazioni per computer e cellulari che riguardano la religione islamica.

Questo breve post è dedicato agli amici della comunità musulmana italiana che mi hanno chiesto dove poter trovare dei programmi per avere sempre a disposizione sui loro computer e tablet il testo sacro della religione islamica, il Corano(alquran).

Su internet, possiamo trovare milioni di pagine scritte in ogni lingua che riguardano l'Islam, ma per una maggiore comprensione per tutti i non arabi praticanti che si avvicinano alla cultura islamica, oggi vorrei presentare alcune applicazioni importanti che possono essere installate su diversi dispositivi e diversi sistemi operativi tra cui GNU/Linux, Windows, Mac, Android.

Iniziamo con la presentazione di un bellissimo progetto Open Source che riguarda proprio lo studio e la comprensione del Sacro Corano(alquran), sono disponibili già da alcuni anni diversi installer per sistemi operativi diversi, dovete fare attenzione solo alla piattaforma che state utilizzando prima di installare i programmi, i386-32, amd64, Mac, Windows.

La descrizione di Zekr la trovate sugli archivi di Sourceforge.net:

"Zekr is an open source Quran study software for Windows, Linux and Mac. It's designed to ease access to the most authentic and valuable text of Muslims. Zekr provides Quran translations, recitation, search and other features to study Holy Quran."

La pagina del progetto Open Source la trovate qui:

http://zekr.org/quran/
questa pagina contiene gli installer per windows

http://zekr.org/quran/en/quran-for-mac
questa pagina contiene gli installer per MacOS

http://zekr.org/quran/en/quran-for-linux
questa pagina contiene gli installer per GNU/Linux

La pagina delle traduzioni è questa:

http://zekr.org/resources.html#translation
dovete controllare la vostra lingua di destinazione e selezionarla nel modo previsto dal programma per applicarla al sistema.

Per scegliere la piattaforma di installazione, scaricando solo il software che vi serve davvero, potete usare questa pagina:

http://zekr.org/download.html
Qui trovate i vari installer per tutti i vostri sistemi operativi.

Se invece volete leggere il Corano in modo diretto e senza scaricare applicazioni che poi dovete installare e configurare, potete leggere il testo sacro direttamente dal web, scegliendo questo link:

http://tanzil.net/#1:1 [Al-Fatiha]

Potete scegliere la vostra lingua per la traduzione istantanea dei vari Aya che compongono le Sura del Corano, potete fare varie ricerche su tutte le pagine disponibili, naturalmente, devo ricordare a tutti che il Corano dovrebbe essere letto nella sua lingua originale, in quanto le traduzioni nelle varie lingue, potrebbero distorcere il significato che hanno nella lingua araba.
Le traduzioni servono a capire il Corano per i non arabi praticanti, ma a volte non rispecchiano quello che il Corano spiega in lingua araba, che può perdere il suo significato se portato in una lingua diversa o

tradotto in un modo non corretto.

A questo scopo, potete usare la pagina degli sviluppatori a questo link:

http://zekr.org/quran/en/develop-for-zekr

Su questa pagina, potete dare il vostro contributo creando nuovi pacchetti linguistici per il progetto, potete partecipare allo sviluppo del programma stesso, potete contribuire a correggere le traduzioni del Corano nelle varie lingue di destinazione, potete segnalare i bug del programma per le correzioni o semplicemente fare domande e commenti oppure richiedere funzioni particolari che vorreste avere sulla prossima release del programma.

Molto bene, ora concludiamo la presentazione per i computer portatili e fissi e passiamo ai dispositivi Android(Tablet/Cellulari).
Come ho specificato all'inizio del post, molti amici musulmani vorrebbero avere almeno il Corano per poterselo portare sempre con loro e poterlo leggere anche senza poter disporre di una connessione internet.
Personalmente, ho potuto scaricare e provare diverse app per la lettura del Corano sui dispositivi Android, e una applicazione in particolare è risultata eccellente sia come traduzione, sia come aggiornamenti e nondimeno come uso giornaliero per la lettura del testo sacro sul mio tablet.

Potete trovare molte app che riguardano l'Islam, dovete pero' vedere quello che vi serve davvero, esistono molte app per gli orari di preghiera, e altrettante per gli sfondi animati per i tablet e cellulari, posso però consigliarvi una bellissima app che potete scaricare per i tablet Android e naturalmente potete avere la traduzione nella vostra lingua se non siete di lingua araba.

Sullo store di Google dovete ricercare questa voce:

Islam: Il Corano
Dimach.Cassiope

La descrizione di questa app è semplice e veloce, questa app è completa e permette di avere sempre una copia del Corano sui nostri dispositivi personali Android(Tablet/Cellulari), l'ultimo aggiornamento risale al 7 aprile 2013 per chi non avesse ancora fatto nessun aggiornamento dalla versione precedente.
Questa splendida app, ci consente di approfondire il Sacro Corano ovunque ci troviamo, in quanto il programma mantiene l'ultima sura letta e ascoltata e quando decideremo di riprendere la lettura, ci riporterà proprio all'ultima parte che abbiamo letto.
Inoltre, i recitatori audio disponibili, possono essere scaricati anche in un secondo momento, se non volete spendere il credito del vostro tablet/cellulare, vi consiglio di scaricare l'audio attraverso una rete wi-fi perchè altrimenti rischiate di consumare tutto il vostro credito cellulare.

La pagina web dello sviluppatore su Google Play la potete trovare a questo indirizzo:

https://play.google.com/store/apps/developer?id=dimach.cassiope&hl=it

Detto questo, auguro a tutti quanti voi una buona navigazione su internet, sperando che questo post possa essere di aiuto agli amici musulmani che mi hanno fatto questa particolare richiesta.

Progetto Graviton: relazioni scientifiche audio e video.

Post n°82 pubblicato il **23 Aprile 2013** da exodus1984
Questo veloce post è dedicato agli amici del progetto Graviton, potete leggere la relazione annuale sulla pagina web di questo blog. :-)

Grazie a tutti per la collaborazione e i consigli tecnici, come sempre, buon divertimento e buona permanenza su internet :-)

Antiche glorie informatiche: i compilatori riportati in vita dalla comunità Open Source.

Post n°83 pubblicato il **24 Aprile 2013** da exodus1984
Carissimi bloggers, oggi parliamo di alcuni programmi che possono essere utili per alcuni utenti di Linux e windows.

Per prima cosa vorrei ricordare un compilatore che ho usato parecchi anni fa e che oggi sembra avere ri-ottenuto una buona diffusione tra gli smanettoni di programmazione avanzata.

Questo compilatore è appunto il FreePascal, che con il progetto correlato, ha praticamente riportato in vita questo linguaggio di programmazione che ormai molti consideravano estinto.

La pagina principale è questa:

http://www.freepascal.org/

Da questa pagina, potete scaricare e vedere gli avanzamenti del progetto, lo sviluppo e i download di units e compiler. :-)

La pagina del download la trovate qui:

http://www.freepascal.org/download.var

La pagina dei contributi per le unit la trovate qui:

http://www.freepascal.org/contrib/contribs.html

mentre per la documentazione in PDF e HTML la potete scaricare da qui:

http://www.freepascal.org/docs.var

E per completare il tutto, per finire in bellezza, qui potete trovare l'IDE di creazione e compilazione visuale per il FreePascal:

http://www.lazarus.freepascal.org/

Se volete seguire l'avnzamento di Lazarus, potete linkare questa pagina:

http://wiki.lazarus.freepascal.org/Roadmap

Passiamo ora ad un altro gioiello della programmazione, anche lui morto e poi rinato grazie all'interessamento dei programmatori Open Source: il leggendario compilatore multipiattaforma Watcom. :-)

Potete vedere il progetto a questo link:

http://www.openwatcom.org/index.php/Main_Page

I suoi manuali in formato PDF li trovate a questo link:

http://www.openwatcom.org/index.php/Reference_Manuals

per scaricare i compilatori dovrete linkare questa pagina:

http://www.openwatcom.org/index.php/Downloads

Qui potete trovare diversi mirrors e diversi sistemi operativi tra i più usati, vecchi e nuovi.

infine, il Freebasic, che ho usato moltissimi anni fa per programmare sistemi di calcolo per il gioco del lotto e vari... ;-))
Lo potete scaricare a questo link:

http://sourceforge.net/projects/fbc/files/

Cari bloggers anche per oggi è tutto, buon divertimento e buona navigazione su internet. :-)

La violenza non serve a nulla: l'Italia vista dalla gente comune.

Post n°84 pubblicato il **02 Maggio 2013** da exodus1984
Carissimi bloggers, oggi vorrei spendere due parole al riguardo degli ultimi fatti di cronaca accaduti in Italia.

Ho scritto questo post per chiarire alcuni aspetti che tutti noi ormai conosciamo sulla politica, sul governo, e sull'economia, ma principalmente per far capire a molte persone che l'uso della violenza può arrecare un serio danno a tutto il popolo italiano, voglio dire che se siamo messi male, non dovremmo certo cercare di andare ancora in peggio...

Negli ultimi anni, ho raccolto informazioni da varie fonti, che proprio al riguardo della situazione economica e politica dell'Italia, mi portano ad elencare alcune semplici parole:

"disastro nazionale"
"bombe"
"armi"
"attentati"
"lotta armata"
"guerra civile"

Allora, una piccola lista di questo tipo, potrebbe portare al crollo definitivo di una grande nazione come l'Italia?

Io credo di no, lo so, la situazione economica è durissima, ma non penso che per questi motivi si debbano portare a termine atti di violenza che vanno contro gli interessi stessi di tutto il popolo italiano.

Ho ascoltato "campane" diverse, ognuna con la stessa musica, allora, perché non seppellire l'ascia di guerra e cercare di risolvere la situazione italiana in modo proficuo e pacifico che tenga conto dei reali bisogni dei cittadini italiani?

Il divario tra politica e cittadini è sempre più grande, a risentirne è l'economia che ripercuote i suoi effetti sui cittadini italiani, allora, perché non cercate di andare d'accordo per salvaguardare la mia povera Italia???

In questo caso, potrei dire migliaia di cose, ma lo sopo di questo post è solo quello di far riflettere la moltitudine di persone che come proposto da altri portali e blog qui sul web, "seminano vento con l'intento di raccogliere tempesta"...

La mia povera Italia non può finire così...

Cari bloggers, anche per oggi è tutto, ho voluto condividere con voi il pensiero che mi sono fatto parlando con persone diverse della odierna situazione economica e politica italiana cercando di comprendere alcune possibili soluzioni.

Mi auguro che alcune persone riflettano su questa situazione, e trovino un accordo valido che riporti il mio grande paese alla dignità che aveva un tempo...

Sistemi di recupero per Windows: creare CD/DVD bootabili per la scansione dei sistemi.

Post n°85 pubblicato il **12 Maggio 2013** da exodus1984
Carissimi bloggers, oggi parleremo di alcuni sistemi per il recupero effettivo di sistemi operativi Windows.

Iniziamo con l'analisi di un piccolo sistema operativo basato su Linux Knoppix che ci consente di scannerizzare il sistema windows posto sotto analisi alla ricerca di malware e virus, nonché di alcuni difetti di bootloader dello stesso.

Prima di iniziare le operazioni di pulizia del vostro sistema Windows, dovrete scaricarvi l'immagine .ISO da masterizzare e lanciare in memoria prima del caricamento del sistema operativo windows.

L'immagine che dovrete scaricare è un freeware e viene definita dal nome della singola versione:

F-Secure Rescue CD 3.16.52606

dopo la masterizzazione della suddetta immagine avremo un CD contenente due directory ben distinte:

boot KNOPPIX

Il sistema può trattare sistemi operativi basati su Windows, in quanto ricerca alcune directory specifiche per il suo funzionamento corretto.

Ora analizzeremo in generale come sia possibile salvare un computer compromesso da virus e malware su cui girano sistemi operativi Windows.
Con questa semplice guida, vorrei fornire anche alle persone non troppo portate con la tecnologia informatica, delle indicazioni con le quali si possono risolvere il 99% dei problemi di avvio e recupero per i vostri sistemi operativi Windows compromessi.

Iniziamo ad elencare le possibili soluzioni a questi problemi:

Bitdefender:
---
http://download.bitdefender.com/rescue_cd/2013/
bitdefender-rescue-cd.iso
masterizzate l'iso e fate partire il sistema prima di windows.

Kaspersky Rescue Disk:
---
download1uk.softpedia.com/dl/c45cd8abc27d3c2a82cea6034de66702/518fecdd/100100454/software/antivirus/kav_rescue_10.iso

PandaSecurity:
---
www.pandasecurity.com/resources/tools/SafeCD.iso

Avira Rescue System:
---
http://www.avira.com/en/download-start/product/avira-antivir-rescue-system?x-origin=web

MicroWorldSystems:
---
http://www.microworldsystems.com/download/tools/escanrd.iso

Microsoft:
---

http://microsoft-standalone-system-sweeper.en.softonic.com/

Questo programma crea un cd/dvd bootabile per la ricerca di virus, malware e rootkit, può essere inserito su una key usb per la scansione portatile dei sistemi operativi Windows. :-)

Gdata security bootCD:
---
download1us.softpedia.com/dl/c7ccbad8961667da90c4a7eae1da6a6e/518ff06c/100172207/software/antivirus/GBR_R_FUL_2012_BootCD.iso

Vba Rescue:
---
ftp://anti-virus.by/pub/vbarescue.iso

Controllo versione FTP:
ftp://anti-virus.by/pub/

Pctools:
---
download.pctools.com/mirror/AOSS-src.tar.gz
la release sorgente, tutta da spippolare... :-))

file .iso:
---
download.pctools.com/mirror/AOSS.iso
attenzione alla release, in LAB mode, con riserve e bug.

Acronis Scan Security:
---
download.acronis.com/iso/AcronisAntimalwareScanCD.iso

E per ultima ma non meno importante, la iso di Ubuntu:

Ubuntu-MRT-v1-2.iso (599.9 MB)

Cari bloggers, anche per oggi è tutto, spero che questi semplici link possano aiutarvi a riportare in vita i vostri sistemi Windows compromessi da virus, malware e rootkit vari. :-)
Come sistemi di sicurezza sono molto validi, visto il loro uso come punto di partenza prima del sistema operativo Windows.
Adesso, spetta a voi usarli nel migliore dei modi per salvare la vita a tutti i computer che portano il sistema Windows, un modo come un altro per riportare in vita un PC compromesso.... ;-))

Buon lavoro a tutti voi :-)

Hardware per smanettoni informatici: i computer SBC.

Post n°86 pubblicato il **31 Maggio 2013** da exodus1984
Carissimi bloggers, oggi inizieremo a conoscere alcune particolari soluzioni hardware che interessano molto agli smanettoni informatici. :-))

Per ora, inizieremo a conoscere alcuni dei principali produttori di SBC, ovvero Single Board Computer, possiamo iniziare con il famosissimo Raspberry-PI, poi troviamo la Embest che produce particolari SBC basati su architettura ARM, quindi la Olimex che produce gli "OlinuXino", SBC molto compatti e preparati per lo studio applicativo dei sistemi, e per ultime, ma non meno importanti, Texas Instruments e Bluetechnix, con architettura basata sempre su ARM. :-)

Ma la lista non finisce certo qui, in quanto stanno nascendo un po dappertutto, aziende che producono SBC a bassissimo costo per l'utente finale, e per la gioia immensa di noi poveri smanettoni. 8-))

Detto questo, credo che sia utile fare una breve presentazione della tanto discussa piattaforma ARM.

Procediamo con ordine, che cosa si intende per processori ARM??? :-)

Ecco una breve panoramica: Atmel, Sun-Microsystems, Toshiba, Raspberry-PI...

Si tratta di processori RISC, ovvero di tecnologia che permette di eseguire istruzioni in modo semplice e veloce rispetto alle cpu CISC che hanno un set di istruzioni più complesse e per cui si richiede al processore del lavoro in più per elaborarle.
Questa semplice spiegazione tecnica è ridotta all'osso proprio per permettere a più persone possibili di comprendere cosa si nasconde alla base dei processori ARM e la differenza con piattaforme standard basate su X86.

Se la nostra amica Samsung manterrà le promesse per il 2014, avremo a disposizione computer in tecnologia RISC a 64 bit grandi quanto una carta di credito, potrete solo immaginare i salti di gioia che farò quando potrò averne uno sotto mano da spippolare... 8-))

Bisogna ricordare agli utenti che siamo già stati "invasi e colonizzati" dai processori ARM, anche se nessuno se ne è accorto fin'ora... ;-)))
Infatti questi processori li troviamo praticamente ovunque, nei tablet, nei cellulari, e molti altri dispositivi che usiamo ogni giorno senza pensare troppo a cosa si muove all'interno dei nostri amati dispositivi elettronici... :-))

Parleremo in seguito anche dei sistemi operativi che vengono usati su questi SBC, di cosa si può fare e dei loro utilizzi particolari per risolvere alcuni problemi legati alla connettività internet, vedremo come gestire una distribuzione Linux e come usarla per costruire un desktop-TV, o un media center come piace a noi. :-)

Un esempio interessante, alimentando un dispositivo ARM tramite un piccolo pannello solare con dimensioni 90x40x10, si può ottenere un perfetto sistema per l'assalto informatico(pen-test) su reti di varia natura usando distribuzioni GNU/Linux preparate appositamente per l'evento... 8-)

Sto preparando della documentazione elettronica in merito a quello che possono realmente fare questi dispositivi ARM, e devo dire che la cosa è estremamente interessante, presto potrò inserirli nella pagina web del blog a disposizione di tutti gli utenti interessati.

Cari bloggers, per oggi è tutto, questa prima introduzione, ci porterà a capire e programmare il nostro SBC per risolvere i problemi che si presentano per la gestione di un valido sostituto ai nostri vecchi computer(portatili/fissi).

Backup e configurazione su Raspbian

Post n°88 pubblicato il **02 Giugno 2013** da exodus1984
Carissimi bloggers, oggi proviamo a fare qualche configurazione semplice per le distribuzioni ARM.

Analizzeremo pertanto la famosissima distribuzione Raspbian.
La prima impostazione che dovete fare è quella di portare la vostra tastiera nella configurazione italiana:

Montate sul vostro sistema Linux la seconda partizione dove è contenuto il sistema completo:
/dev/sdd2 on /media/62ba9ec9-47d9-4421-aaee-71dd6c0f3707 type ext4 (rw,nosuid,nodev,uhelper=udisks)

ora dovete editare il file /etc/xdg/lxsession/LXDE/autostart
Ecco una breve descrizione del suo contenuto:

Raspbian originale LXDE:

@lxpanel --profile LXDE
@pcmanfm --desktop --profile LXDE
@xscreensaver -no-splash

Raspbian modificato per noi poveri smanettoni italiani... ;-))

@setxkbmap -option grp:switch,grp:alt_shift_toggle,grp_led:scroll it,us
@lxpanel --profile LXDE
@pcmanfm --desktop --profile LXDE
@xscreensaver -no-splash

ora passate alla prima partizione della SDcard:

/dev/sdd1 on /media/C522-EA52 type vfat
(rw,nosuid,nodev,uhelper=udisks,uid=1000,gid=1000,shortname=mixed,
dmask=0077,utf8=1,showexec,flush)

In questa partizione, editate il file config.txt e modificate la riga per l'HDMI:

originale:
uncomment to increase signal to HDMI, if you have interference, blanking, or
no display
#config_hdmi_boost=4

modificato:
# uncomment to increase signal to HDMI, if you have interference, blanking, or
# no display
config_hdmi_boost=4

Ho avuto qualche problema con il cavo HDMI da 5 metri, e questa opzione ha risolto la situazione in modo ottimale per effettuare i test.

La tastiera standard che ho installato su Raspberry è la classica Logitech K400, mentre per la connessione internet ho installato il Nano Dongle della Digicom 150N una key wireless che viene riconosciuta da Raspbian e poi configurata correttamente.

Ora, salvate i file, smontate la SDcard e caricatela sul vostro RaspBerry-PI per vedere in azione le modifiche fatte.
Ho caricato alcune schermate di Raspbian in azione, potete vederle cliccando sulla barra di navigazione di Libero ovvero su "FOTO", per vedere gli album fotografici dei sistemi operativi. :-)

Backup da Linux per sistema Raspbian:

Una volta aggiornata la vostra Raspbian con la prima connessione internet,
dovete assolutamente salvare una immagine di recupero(vi servirà...).

Inizierò a spiegare un semplice backup da terminale, usando il programma
copyraw.
Montate la SDcard con Raspbian in una distribuzione Linux(es.Debian...),
quindi elencate i punti di montaggio della scheda sul vostro sistema Linux in questo modo:

root@exodus84:/home/enrico# mount
Al termine del mount, dovrete trovare le due partizioni di Raspbian:

/dev/sdd2 on /media/62ba9ec9-47d9-4421-aaee-71dd6c0f3707 type ext4
(rw,nosuid,nodev,uhelper=udisks)
/dev/sdd1 on /media/C522-EA52 type vfat
(rw,nosuid,nodev,uhelper=udisks,uid=1000,gid=1000,shortname=mixed,
dmask=0077,utf8=1,showexec,flush)

Ora potete crearvi una immagine di backup della vostra SDcard su disco fisso usando il programma
copyraw come segue:

La shell vi ritorna questo errore:
bash: ./copyraw: Permission denied

Rendete eseguibile copyraw con questo comando:
root@exodus84:/home/enrico# chmod 755 copyraw

Quindi iniziate la clonazione dell'immagine da SDcard

root@exodus84:/home/enrico# ./copyraw /dev/sdd /home/enrico/raspbianIT262013.img

Questa è la schermata iniziale del programma:

CopyRAW v.6.3 - Created by EnriKo 1983-2006(R) - Italy -
Inizio Operazione di Recupero, copia RAW_BYTE in Corso.....
Chiusura File_DEV: Destinazione e Sorgente OK!!!

SE non ci sono problemi dovuti ai supporti fisici, il programma dovrebbe
terminare correttamente:

Quando CopyRAW non sembra funzionare:
```
 ########################################
 [ Aiuto_1:                                ]
 [ Non sei loggato come user             ]
 [ percui non puoi usare i Socket RAW.   ]
 [ CopyRAW e' stato pensato per il        ]
 [ recupero dati, percui richiede i       ]
 [ permessi di lettura e scrittura        ]
 [ a livello amministrativo.               ]
 [----------------------------------       ]
 [ Aiuto_2:                                  ]
 [ Prova ad usare                           ]
 [ registrandoti nel file:                  ]
 [ /etc/sudoers.                            ]
 ########################################
```

>>>> Operazione di Copia RAWbyte riuscita. <<<<
CopyRAW v.6.3 - Created by EnriKo 1983-2006(R) - Italy -

Con un comando del tipo ls -la *img potete controllare il recupero effettivo
della vostra immagine da SDcard, in questo caso ecco l'uscita finale di
copyraw:

root@exodus84:/home/enrico# ls -la *img
-rw-r--r-- 1 root root 3947888640 2 giu 14.21 raspbianIT262013.img

Cari bloggers per oggi è tutto, il programma di clonazione "CopyRAW" lo potete scaricare dalla pagina WEB dedicata di questo blog, cliccando su "SITO" nella barra di navigazione di Libero posta qui sopra, ho messo a disposizione anche la versione compilata per ARM per un suo utilizzo futuro. :-)

Raspbian: Ridimensionare le partizioni per usare una SDcard da 8Gb.

Post n°89 pubblicato il **08 Giugno 2013** da exodus1984
Carissimi bloggers, oggi parleremo della riconfigurazione delle partizioni sul sistema operativo Raspbian.

Ma partiamo con ordine... ;-)))

Il sistema Raspbian viene fornito di default su una SDcard da 4GB, questo ci porta inevitabilmente prima o poi ad esaurire lo spazio disponibile su questo dispositivo di archiviazione e qui cominciano i nostri primi problemi...;-)))

Come test principale, ho preferito fare chiarezza sul metodo di ridimensionamento del sistema operativo Raspbian, in quanto la mancanza di spazio per poter installare altri programmi che mi servivano, mi ha fermato la creatività per alcuni giorni, durante i quali ho potuto riflettere sulle possibilità applicative che vorrei fare con i miei RaspBerry-PI. :-))

Ecco qua la procedura:

selezionate la partizione della SDcard indicata da Gparted (/dev/sdd2...)
Quando la partizione viene selezionata, cliccate su: "Ridimensiona/Sposta" e tenendo premuto il tasto sinistro del mouse sugli indicatori a freccia della partizione selezionata, "allungate" le dimensioni originali(3,9Gb) al totale di 7,42Gb per la nuova scheda SDcard(8Gb).
Per ora 8Gb ci bastano, ritorneremo sull'argomento quando avremo finito anche questi pochi GB... ;-)))

Gparted provvederà quindi a reimpostare sia il filesystem EXT4 che al ridimensionamento per la nuova scheda che avrete comprato in precedenza per aumentare lo spazio operativo per l'installazione di nuovi programmi sulla vostra Raspbian.

Al termine di questa banale operazione, vi ritroverete con uno spazio EXT4 doppio rispetto alla SDcard da 4 Gb in cui Raspbian girava in modo molto ristretto, informandovi parecchie volte con il solito messaggio di "disk full", impedendovi di installare ulteriori software dal repository. 8-))

Ecco un breve riassunto della procedura che ho fatto con la mia Raspbian:

1) Salvate una immagine completa dalla vecchia scheda SDcard da 4GB.
2) inserite la nuova SDcard da 8Gb nel lettore.
3) aprite un terminale e digitate il seguente comando:

3-1) ./copyraw raspbian5giugno2013.img /dev/sdd

oppure per chi non dispone del copyraw, usate il comando "dd":

3-2) dd if=raspbian5giugno2013.img of=/dev/sdd bs=4M

Ricordate sempre di dare un comando sync al termine di questi programmi per il semplice ma importante motivo di finalizzare correttamente la scrittura sulla vostra SDcard(4Gb), naturalmente, dovrete attendere anche il termine del comando sync prima di togliere fisicamente la SDcard dal lettore...!!!(cercate di non distruggere tutto...) ;-)))

4) ora vi ritrovate con le partizioni della SDcard da 4Gb su una SDcard da 8Gb, per cui vi rimane uno spazio vuoto da circa 3,9Gb non allocato...

5) lanciate il programma Gparted da un terminale aperto e aggiornate i dispositivi.

6) Da Gparted, selezionate la partizione da 3,9 Gb e quindi cliccate su "Ridimensiona/Sposta", quando vi appariranno le frecce sulla partizione, potrete ridimensionarle per i restanti 3,9Gb, ottenendo così una nuova partizione da circa 7,50 Gb, che il programma Gparted provvederà a formattare in Ext4 per voi. :-)

7) Al termine di tutto questo spippolamento, togliete la SDcard dal lettore inseritela nel vostro fedele RaspBerry-PI e date fuoco alle polveri...:-)

Questa procedura, può sembrare complicata, ma vi posso garantire che viene conclusa nel giro di pochi minuti, ho scelto il programma Gparted proprio per l'uso grafico che può essere usato anche dai neofiti che non hanno dimestichezza con i terminali di testo.

Adesso possiamo giocare seriamente con i nostri RaspBerry-PI ;-))

Alcuni esempi pratici?

Server Web statico, Ftp, server criptato, tutti quanti come sempre su rete Wi-Fi locale, disponibile per tutti gli utenti locali(siamo in 4 gatti...).
E queste sono solo alcune banali applicazioni utili che un RaspBerry-PI potrebbe fare, ma siccome gli spippolamenti sono molteplici e diversi tra di loro, tanto per iniziare, ho pensato solamente a quelle che possono essere usate dai miei utenti locali... ;-))

Per finire questo breve post, ho messo alcune foto del ri-partizionamento sui server di Libero, in modo che siano accessibili a tutti voi per vedere e comprendere meglio questa procedura.

Con questo post, concludiamo anche la prima parte delle spiegazioni tecniche che ci servono ad avere sempre più spazio operativo e sempre più applicazioni installate sul nostro RaspBerry-PI.

Cari bloggers, buona navigazione a tutti voi, e buon divertimento su internet.

Il misterioso mondo delle reti "oscure"... viaggio informatico negli abissi di Internet :-)

Post n°91 pubblicato il **22 Giugno 2013** da exodus1984
Carissimi bloggers, ri-eccoci qui a ri-parlare del sistema Tails. :-))
Oggi analizzeremo le reti criptate e i loro derivati per capire e comprendere la reale utilità di usare un sistema "anonimo" per la nostra navigazione su internet.

Allora, iniziamo a spiegare che cosa può essere un "sistema operativo anonimo", moltissime persone, credono ancora oggi che internet sia una unica grande rete di computer dove si possa trovare di tutto e di più...:-)

In teoria, questa banale denominazione, viene compresa un po da tutte le persone che oggigiorno sono perennemente connesse ad internet, però in pratica, le cose non stanno proprio così...:-))

Internet si divide inizialmente in due grandi blocchi, il primo blocco è appunto quello che utilizziamo tutti quando ci connettiamo alla rete e visitiamo i siti web che ci interessano di più, il secondo grande blocco è invece costituito dalle cosiddette "darknet", ovvero reti e sistemi "anonimizzati" da sistemi operativi e hardware specifico per rendere impossibile il tracciamento di questi utenti che usano questa parte di internet, infatti, molti amici che conosco, definiscono questa parte di rete il vero "underground" della rete internet mondiale.

Avendo compreso questo primo e banale concetto sulla vera natura del traffico che può essere instradato sulla normale rete internet, adesso cercheremo di approfondire un argomento che non è noto a tutti i "normali" utenti, che pensano appunto di navigare su internet tra "rose e fiori"...;-))

Le reti appartenenti al secondo blocco, forniscono servizi anonimi e criptati che vengono usati principalmente da organizzazioni di vario tipo(militari, criminali, terroristi, pedofili, mercenari e killer).
Ma a noi, tutto questo non interessa, in quanto quello che ci preme di più è capire se questi servizi cosiddetti "anonimi", possano davvero esserci utili oppure in caso contrario, utilizzare altri sistemi.

Ora che abbiamo fatto chiarezza su quello che si nasconde dietro alla rete che tutti noi utilizziamo ogni giorno per lavorare e per divertirci possiamo passare alla domanda da un milione di euro:

Siamo davvero anonimi su queste reti??? :-=))

La cifratura fornita dalla rete Tor(Mister Cipolla...) è definita molto buona da alcuni volponi informatici di mia conoscenza, e quindi mi si è acceso un led in testa(una volta c'erano le lampadine...), ho avuto subito un'idea pazzesca, un inseguitore di identità cifrate....8-)

Come tutti ben sapete, con il sistema Tails abbiamo la possibilità di ottenere migliaia di nuove identità nel corso di una unica sessione cifrata, identità cifrate che cambiano quando volete voi oppure per un tempo prestabilito dalla configurazione di rete.

La versione che è stata utilizzata durante questo test, è la 0.18, il test è stato condotto usando i parametri originali della stessa distribuzione, quindi non è stato necessario modificare la ISO del sistema aggiungendo i moduli per un test di assalto alla rete criptata.

Ma torniano alla nostra domanda di base, QUANTO sono sicuri questi sistemi per un utente "normale" che voglia provare l'ebrezza di essere "anonimo" in rete???
La risposta globale sarà quindi, "buona" per la maggior parte, ma personalmente, non userei mai un sistema di questo tipo per navigare

sulla rete.
Però qui la mia opinione personale, non conta, perché uso altre reti e altri sistemi che non mi rendono "dipendente" ne da queste reti, ne da questi sistemi.

Quindi, un utente normale che voglia provare un sistema di questo tipo, si deve rendere conto che affida la sua privacy ad un sistema che magari non comprende bene, per cui, è tutto contento solo perché il sistema operativo che sta usando è "anonimo", ma nel frattempo, non si rende conto che alle porte del suo computer, stanno bussando numerosi tapiri informatici... :-))

Il consiglio che vi posso dare se volete testare seriamente uno di questi sistemi operativi, è questo:

1) usate un computer senza disco fisso ma con almeno 4 Giga di memoria ram

2) modificate la distribuzione che avete scelto e installateci i vostri software di difesa(vi saranno utili...)

3) usate con preferenza un PC portatile, essendo dotato di batteria, eviterete un riavvio involontario dovuto alla mancanza di corrente elettrica, anche se certi riavvii, sono possibili dalla rete "anonima" stessa(ma non avevate cambiato la vostra identità per la centesima volta???)...:-)))

4) non cercate guai su queste reti, ci sono diverse unità informatiche appartenenti ai signori che ho elencato in precedenza, che possono trovarvi in pochi secondi...8-))

5) Ricordate sempre che siete "cifrati" ma non "anonimi", e la rete Tor non può certo garantire l'anonimato assoluto, ma qui parlo solo per esperienza personale dovuta a migliaia di spippolamenti strani su questo tipo di rete....:-)

Esistono migliaia di reti "oscure", e quelle veramente speciali, non le trovate certo su internet, per cui, fate molta attenzione, le reti "anonime" nascondono molte verità sconosciute agli utenti normali che si avventurano da soli in questo far-West informatico, qui troverete cose che fanno sembrare la razza umana simile ad una bestia inferocita, senza un briciolo di umanità verso cose e persone...:-(

I test che ho condotto usando questa versione di Tails, hanno dato i risultati cercati, sono stati creati rispettivamente due tunnel, uno come client e l'altro come server per gestire un sito "anonimo".

Potete vedere tutta la procedura guardando le foto della sessione cifrata che comprende i due sopracitati tunnel attivi e usati da diverse "entità" molto particolari ai due emisferi del pianeta...
(test killing.gov e darkweapons) 8-))

Potrete vedere anche la pagina per la creazione di web-server anonimi, le spiegazioni sono molto semplici e alla portata di tutti i naviganti "cifrati".

Le reti "oscure", fanno parte di internet ormai da molto tempo, la nostra società tecnologica e informatica ha ricreato la vita reale, ma gestita in modo elettronico e del tutto uguale a quello che potreste trovare appunto nella vostra vita reale, organizzazioni di vario tipo navigano nelle acque dei fondali di internet, ma tutto questo serve anche per il controllo globale di situazioni economiche e politiche, questo è il posto ideale per ottenere servizi particolari senza che un'organizzazione conosciuta, possa sporcarsi le mani in modo diretto...
Questo è il nuovo mondo virtuale dove "la Legge perdeva l'impero"... ;-))

Per concludere questo breve post, ho messo alcune immagini del test eseguito sulla rete criptata sui server di Libero, come sempre, sono accessibili a tutti voi cliccando su "FOTO" qui sopra sulla barra di navigazione del blog, e spulciando l'album "anonymous". :-)

Queste immagini mostrano il test iniziale usando il camuffamento del sistema Linux Tails come sistema operativo Windows XP, funzione utile se usate il portatile in pubblico dove ci sono molte persone che guardano il vostro schermo....:-)))

Detto questo, cari bloggers, approfitto del post per salutare e ringraziare gli amici di rete per le informazioni tecniche fornite, e naturalmente un saluto e un augurio a tutti quanti voi per una buona navigazione "anonima"...;-)))

007 italiani cercasi: quando la Patria chiama. :-)

Post n°92 pubblicato il **10 Luglio 2013** da exodus1984
Carissimi bloggers, oggi vorrei dedicare questo post ai futuri 007 italiani.

Come tutti ben sapete, la voglia di mettersi in gioco di ragazzi e ragazze con in mano una laurea, è molto forte in questo periodo, va da se che anche la crisi economica spinge le persone ad accettare qualsiasi posto valido, ma se la richiesta arriva nientemeno che da un organismo istituzionale italiano, allora è il caso di provarci.

Molte persone infatti, spediscono i loro curriculum nella speranza di essere selezionati, ottenendo così un lavoro sicuro, ben pagato e di alta qualità.

il sito istituzionale www.sicurezzanazionale.gov.it, offre proprio quello che cercano i giovani laureati, e quindi potete inviare le vostre richieste a questo sito, cliccando su "lavora con noi" e poi su "inviaci il tuo curriculum", la richiesta dei vostri dati è valida fino al 31 ottobre alle ore 12.00, il sistema di acquisizione online provvederà a tutto.

Alcuni amici mi hanno chiesto il perché di un post di questo tipo, ed eccovi la risposta pubblica: amo il mio paese, ma per motivi diversi non posso partecipare a queste selezioni, quindi ho scritto questo post per dare la possibilità a chi non ne fosse al corrente, di poterlo fare, approfittando di questa occasione. :-)

Ma torniamo al post in questione, molti bramano un posto di questo tipo, ma siete davvero pronti a farlo??? :-))
Quello che voglio dire è che ho davvero visto troppe cose, e forse i nuovi 007 italiani non si potrebbero adattare a certe situazioni strane...;-)))
Per valutare tali rischi, ho inviato una striscia a fumetti per capire la Cyber-Intelligence, la potete trovare come sempre cliccando sulla barra di Libero qui sopra il blog su "FOTO", poi dovrete cliccare su "A.C.K.ErrH" per vederla. :-)))

la striscia a fumetti "A.C.K.ErrH", è stata creata una sera di tanto tempo fa in un bar, mentre con alcuni amici, si stava discutendo proprio di informazioni riservate...(solo un caso?...) ;-)))
Potete vedere ancora l'impronta del cappuccino preso quella sera come prova...;-)))

Va bene, per oggi è tutto, approfitto del post per salutare i "ragazzi" della sicurezza nazionale e per augurare a tutti quanti una buona navigazione in rete e buona fortuna con le selezioni...:-))

Rimozione ricerca dalla pagina Web.

Post n°93 pubblicato il **21 Luglio 2013** da exodus1984
Carissimi bloggers, oggi invio questo breve post allo scopo di chiarire alcune situazioni intervenute durante il tempo di pubblicazione del video che riguarda una ricerca condotta in prima persona assieme ad altri colleghi ed amici.

Da una decisione presa in accordo con altre persone, viene rimossa la documentazione inviata sulla pagina web fornita dai server di Libero.it e il video dal canale Youtube che ha portato tante ombre negative su questa ricerca durata diversi anni.

I motivi che hanno portato a tale decisione, sono dovuti al mantenimento della pace interiore delle persone che hanno collaborato a questa ricerca e che si sono viste trattate come dei volgari truffatori.

Pertanto, in accordo con la decisione presa, vengono rimossi dalla rete i documenti in PDF e il video riguardanti la sopracitata ricerca, e verranno contestati i documenti e le copie del video rimesse in rete senza una regolare autorizzazione scritta.

Concludo augurando a tutti un buon proseguimento su internet, e come sempre, un buon inizio settimana per tutti quanti voi.

La Scienza e la Fede verso l'infinito.

Post n°94 pubblicato il **23 Luglio 2013** da exodus1984
Carissimi bloggers, oggi voglio proporre un argomento che forse molti di voi non potrebbero approvare pienamente, ma rispetto la volontà e la libertà di tutti, e quindi rimetto a voi la sentenza finale di questo semplice post.

Negli anni passati la fede ha fatto girare il mondo nel bene e nel male schiacciando tutti i tentativi individuali di portare avanti una filosofia e uno spirito di libertà che avrebbero permesso all'intera umanità di progredire e (forse) di poter diventare migliore di quello che è stata negli ultimi 2000 anni.

Quello che intendo dire è che molte informazioni strategiche hanno portato ad un declino quasi totale di questo mondo, nel senso che le persone non sono più unite dallo stesso spirito con cui erano unite nei secoli passati, il controllo informativo ha reso le persone più diffidenti, per esempio, se il vicino di casa lavora fino a notte fonda allora si insinua subito il sospetto di qualche attività illecita o fuori dal comune senso civico nei vicini di casa che devono essere sempre aggiornati su tutto quello che succede vicino a loro...

Per cui, la menzogna, il discriminare liberamente le attività delle persone per potersi impadronire dei loro tesori o segreti, il mondo in cui viviamo, ha perso la propria fede, e tutto quello che è rimasto è solo una inutile corsa al consumismo...

Ma tornando al post in questione, la discriminazione è il peggiore male che l'umanità abbia mai inventato nel corso di tutta la sua storia, è forse questo che siamo destinati a diventare? Sciocchi egoisti senza un briciolo di pietà verso niente e nessuno?

La fede in quello che crediamo, (in questo caso non in Dio) ci aiuta a superare barriere ritenute impossibili nella nostra vita, e da quello che vedono le altre persone, possiamo risultare folli o essere fatti oggetto di discriminazione nel lavoro e nella vita, solo perché le persone che ci guardano non riescono ad avvicinarsi al nostro modo di pensare e di operare nella più completa libertà di pensiero e di azione di cui possiamo farci carico a livello personale.

La fede nella scienza, un punto critico e dolente di molti ricercatori indipendenti che hanno preferito non seguire i dettami della cosiddetta "scienza ufficiale", e vengono quindi "discriminati" dai colleghi che sono appunto diventati famosi seguendo i rigidi dettami di una scienza datata che non lascia spazio alle idee molto spesso rivoluzionarie solo perché potrebbero offuscare se non distruggere la scienza definita "unica e ufficiale", vale a dire: o sei con noi o contro di noi...

Nel Sacro Corano (Sura XXV, 31, Al Furquan, il discrimine), si trova tutta la saggezza che descrive la malvagità umana nei confronti dei propri simili:

"Ad ogni profeta assegnammo un nemico scelto tra i malvagi, ti basterà il tuo Signore come guida e ausilio".

Insh'Allah.

Questo semplicissimo versetto, incorpora tutta la conoscenza del sapere concesso all'umanità, per cui, da pensatore libero e senza nessun vincolo di leggi fisiche e umane, lo scrivo direttamente qui per tutti voi su questo semplice blog perché possiate davvero pensare con la vostra testa senza essere prigionieri di dettami scientifici, religiosi e di natura umana contraria al vostro reale modo di pensare.

Con questo semplice post, ho voluto ribadire ancora una volta lo spirito di libertà e di pensiero per il quale molte persone mi hanno criticato per il mio lavoro scientifico "non ufficiale", per cui a tutte queste persone, posso solo augurare di aprire la propria mente per poter viaggiare liberi verso l'infinito.

Cari bloggers, concludo questo post lasciandovi riflettere liberamente su quanto è stato scritto oggi su questo piccolo blog, e naturalmente auguro a tutti quanti voi una buona permanenza su internet.

Tempo, Spazio, Gravità, e molto altro ancora ... :-)

Post n°95 pubblicato il **03 Agosto 2013** da exodus1984
Carissimi bloggers, oggi vorrei chiarire per tutti gli amici che mi conoscono a livello personale, un argomento che ha tenuto banco tra gli addetti ai lavori per una settimana... ;-)

Dunque, facendo riferimento agli ultimi eventi accaduti, ho deciso di scrivere questo breve post per cercare di portare un po di luce su alcuni effetti previsti e non previsti al riguardo del tanto contestato Progetto DeGraviton.

Descriverò in breve la struttura della materia, così come la conosciamo e come viene indicata nei testi della fisica ufficiale:
le prime ipotesi sulla struttura della materia vennero formulate da un filosofo greco, Democrito di Abdera(IV secolo a.c.)che teorizzò l'esistenza di "mattoni" microscopici in continuo movimento chiamati appunto "atomi", ovvero "indivisibili".

Tuttavia, con le moderne tecnologie, oggi noi sappiamo che gli atomi esistono e che nonostante le continue scoperte sulla divisione atomica rendano chiaro a tutti che "sotto ce' ancora qualcosa...", non possono essere considerati ancora i costituenti fondamentali della materia.
In ogni caso l'atomo rimane per definizione storica, la più piccola parte che possa conservare le caratteristiche chimiche per formare i composti chimici per la produzione di materia (Progetto TransMat).

Ogni atomo è quindi composto da un nucleo, e da un certo numero di elettroni, il nucleo è composto a sua volta da due diversi tipi di particelle subatomiche, i protoni e i neutroni.
Quindi, supponendo che il nucleo atomico abbia le dimensioni di un centimetro, gli elettroni per formare l'atomo, dovrebbero orbitare mediamente ad una distanza di quasi un kilometro dal nucleo del nostro atomo di test, e qui si trovano i primi rudimentali effetti di portanza gravitazionale a livello subatomico che tanto ci interessano.

Quale tipo di energia è mai necessaria per catturare e far orbitare degli elettroni ad una distanza così infinitamente grande sempre tenendo presente che stiamo parlando del nostro ipotetico atomo di test ?

Parliamo allora di una forza estremamente grande, ma racchiusa in qualcosa di infinitamente piccolo che può generare sia una trazione costante che una reazione contraria, in questo caso, il moto di oggetti inanimati che si spostano usando una forza uguale e contraria.
Un semplice e banale esempio, è che se siamo qui sulla Terra, subiamo gli effetti della gravità, ma se ci troviamo nello spazio dove il campo gravitazionale terrestre è sempre presente e minore, potremmo essere soggetti a spostamenti per cui la gravità terrestre non ci farebbe nessuna differenza...

Analizziamo un qualsiasi oggetto inanimato, prendiamo per esempio il classico foglio di alluminio usato ogni giorno da tutti voi per farci cose estremamente diverse ma utili alla vita che conduciamo di solito:

Prendiamo un pezzo di questo materiale, e appoggiamolo su un banale foglio di carta in formato A4, questo pezzo di alluminio è un oggetto inanimato, e non può spostarsi da solo... :-)

Quindi, secondo le leggi fisiche ufficiali, se noi applichiamo a questo corpo una forza, possiamo dimostrare che per questo oggetto, il rapporto

tra forza applicata e l'accelerazione, ha un valore costante per cui le forze sono direttamente proporzionate all'accelerazione prodotta... Questo rapporto costante tra una forza applicata all'oggetto e la sua accelerazione, si chiama "massa inerziale", proprio perché misura l'inerzia, ovvero la resistenza del nostro oggetto nel modificare il suo stato di moto o di quiete(Effetto DeGraviton).

Facciamo un altro banale esempio: il classico libro posto sopra un tavolo, abbiamo la forza gravitazionale che attira il libro, ma questo viene trattenuto dal tavolo che in questo caso esercita una resistenza contraria, le due forze tengono fermo il libro sulla superficie del tavolo senza farlo cadere, per cui abbiamo due forze applicate allo stesso oggetto.

Proseguiamo parlando del moto di oggetti inanimati, la forza gravitazionale è di tipo conservativo/attrattivo, se appunto il nostro foglio di alluminio subisce uno spostamento dovuto ad una forza, si sposterà in direzione della forza(Effetto XDG),ma per cui, che cosa potrebbe essere questa forza che genera un movimento su qualsiasi tipo di materia inanimata?

Quindi posso dire che un magnete sottoposto alla guida d'onda del sistema DeGraviton perde i suoi poli, cadendo verso l'alto, venendo attirato dalla forza(Effetto XDG),per cui se normalmente usiamo delle calamite, possiamo vedere che invertendole, si respingono, mentre questo effetto elimina di fatto la polarità del magnete, attirandolo sempre e comunque in modo inverso al campo gravitazionale della Terra.

Il video riguardante uno dei dieci esperimenti fatti con questo sistema, è stato rimosso dal canale Youtube perché non conforme alle aspettative di qualità che hanno contribuito a dichiararlo un "falso" e quindi è stato rimandato in rete il filmato originale di questo esperimento (659Mb)in HD, rendendolo disponibile solo alle persone autorizzate per la sua visione.
La ricerca, verrà nuovamente inviata sui server ad accesso autorizzato per la definizione del futuro di questo progetto, contestato da tutti, ma da tutti cercato sulla rete.
Credo che il futuro di questo progetto, potrà portare alcuni grandi cambiamenti, il sistema era già stato proposto per il brevetto, ma alcune "voci di corridoio", dicono che purtroppo questa ricerca si fermerà qui per sempre... :-(

Vi sono chiari e lampanti motivi dietro alle voci che si sentono in giro, e quello che posso dire è che esiste davvero qualcosa dietro a tutti questi eventi, posso dire che il video in questione è stato giudicato "interessante" da parte di molti paesi esteri, tanto che alcune statistiche sono state letteralmente e volutamente "cancellate" dai rapporti per coprire l'interesse generato dalla pubblicazione del video verso questo sventurato progetto.

Per cui, in conformità a quanto deciso nei giorni scorsi, il video in HD dell'esperimento originale è stato reso disponibile di nuovo in rete, ma su server ad accesso autorizzato.
Tutti gli esperimenti precedentemente realizzati che erano pronti per la pubblicazione su YouTube, sono stati ritirati in attesa della sorte futura di questo progetto.

Concludendo questo breve post, ringrazio tutti gli amici che sempre mi hanno sostenuto per trovare nuove strade al di fuori dei dettami della scienza conosciuta, e ringrazio tutti quelli che sempre mi hanno detto "questo non si può fare..." mentre io andavo avanti per la mia strada "facendo di tutto e di più"... :-)

Cari amici e cari bloggers, per oggi è tutto, spero di concludere

questa vicenda il più presto possibile per poter tornare a scrivere post di tutt'altro interesse su questo piccolo blog.
Auguro a tutti quanti voi un buon fine settimana e ci rileggeremo più avanti con post un tantino più "leggeri" e "digeribili" di questo.

Il pensiero del Lunedì... ;-))

Post n°96 pubblicato il **01 Settembre 2013** da exodus1984
Carissimi bloggers, oggi finalmente posso riprendere a scrivere qualcosa su questo piccolo blog. :-)

Durante questa caldissima estate, ho avuto modo di riflettere sul futuro degli eventi che governano il mio antico modo di pensare lungo la strada della vita, e durante questo periodo, ho potuto valutare le varie situazioni in un modo diverso dal solito ottenendo dei risultati abbastanza discreti. :-)

E visto che tra poco tutti quanti torneranno al proprio lavoro, io (purtroppo...) dovrò fare altrettanto...;-))
Durante una veloce assistenza informatica di pre-riscaldamento, ho potuto catturare otto virus, rimettendo in funzione un vecchio pc con un sistema operativo WindowsXP.
Questo piccolo lavoretto, mi è servito per scaricare lo stress dovuto ad un periodo di dolce far-niente, dal quale solo adesso riesco a riprendermi... ;-))

Le poche cose che ho fatto qui sul blog, si limitano solo ad alcuni piccoli aggiornamenti della pagina web, ma senza grandi cambiamenti.
Oggi, ho scritto questo post con l'intento di portare una nuova e ricca stagione di articoli che ritengo interessanti e che forse potrebbero essere utili anche ad altri utenti.

Vedremo che cosa ci riserverà il futuro, per ora posso solo augurarvi un buon rientro dalle ferie e una buona navigazione su internet. :-)

Rootkit: i cuccioli sperduti sull'autostrada di Internet... ;-))

Post n°97 pubblicato il **04 Settembre 2013** da exodus1984
Carissimi bloggers, oggi vorrei parlare di un argomento che già conoscete bene, ovvero i rootkit. :-)

Come avevo specificato alcuni post addietro, questi programmi prendono il controllo del sistema dell'utente, lasciandolo lavorare in modo del tutto normale, ma loggando tutto quello che l'utente bersaglio fa sul proprio computer al solo scopo di ottenere varie informazioni che nella maggioranza dei casi, non servono solo a controllare la vita della persona e del computer colpito, ma possono indicare altri tipi di bersagli da acquisire per poter tracciare varie informazioni e scoprire altre macchine collegate in rete.

Sui vari sistemi *nix, Linux compreso, possiamo imbatterci molto spesso in alcuni dei seguenti "cuccioli indifesi", ogni rootkit pertanto, può essere calibrato per il singolo sistema che deve essere attaccato, ma l'uso sempre più pesante di rootkit può avere conseguenze davvero catastrofiche, vediamo una semplice lista dei maggiori rootkit usati per il controllo di reti e sistemi:

55808 Trojan - Variant A
ADM Worm
AjaKit Rootkit
Adore Rootkit
aPa Kit
Apache Worm
Ambient (ark) Rootkit
Balaur Rootkit
BeastKit Rootkit
beX2 Rootkit
BOBKit Rootkit
cb Rootkit
CiNIK Worm (Slapper.B variant)
Danny-Boy's Abuse Kit
Devil RootKit
Dica-Kit Rootkit
Dreams Rootkit
Duarawkz Rootkit
Enye LKM
Flea Linux Rootkit
Fu Rootkit
Fuck`it Rootkit
GasKit Rootkit
Heroin LKM
HjC Kit
ignoKit Rootkit
IntoXonia-NG Rootkit
Irix Rootkit
Jynx Rootkit
KBeast Rootkit
Kitko Rootkit

Knark Rootkit
ld-linuxv.so Rootkit
Li0n Worm
Lockit / LJK2 Rootkit
Mood-NT Rootkit
MRK Rootkit
Ni0 Rootkit
Ohhara Rootkit
Optic Kit (Tux) Worm
Oz Rootkit
Phalanx Rootkit
Phalanx2 Rootkit
Phalanx2 Rootkit (extended tests)
Portacelo Rootkit
R3dstorm Toolkit
RH-Sharpe's Rootkit
RSHA's Rootkit
Scalper Worm
Sebek LKM
Shutdown Rootkit
SHV4 Rootkit
SHV5 Rootkit
Sin Rootkit
Slapper Worm
Sneakin Rootkit
'Spanish' Rootkit
Suckit Rootkit
Superkit Rootkit
TBD (Telnet BackDoor)
TeLeKiT Rootkit
T0rn Rootkit
trNkit Rootkit
Trojanit Kit
Tuxtendo Rootkit
URK Rootkit

URK Rootkit
Vampire Rootkit
VcKit Rootkit
Volc Rootkit
Xzibit Rootkit
zaRwT.KiT Rootkit
ZK Rootkit

Questa semplice lista, serve a farvi capire che la sicurezza informatica può non bastare per fermare chi vuole controllare quello che fate nella vostra vita, attraverso il vostro computer... :-(
Esistono implementazioni di rootkit assolutamente invisibili, ma come si può giungere a questo?
La regola di "non accettare Karamelle dagli sconosciuti" è sempre valida ma in questi casi non può servire proprio a nulla, come dicevo prima, si può usare un sistema e non essere al corrente che qualcuno ci sta controllando per ottenere tutto quello che vuole e desidera da noi, che siamo solo dei poveri e indifesi utenti di internet... 8-)

Allora, come ovviare a tutto questo??? :-))

1) smettiamo di connetterci ad internet...
2) prendete una mazza da carpentiere e uccidete il vostro computer...
3) sto scherzando.... ;-)))

Ritorniamo seri almeno per cinque minuti e riprendiamo il discorso sul post in questione, esistono dei sistemi Live che permettono di rilevare in modo abbastanza corretto le "firme" di questi "cuccioli sperduti" nella rete, offrendo la possibilità agli utenti di scovarli e rimuoverli semprechè non abbiano modificato qualche driver importante per il funzionamento del sistema in uso.

La pagina del progetto la trovate su Sourceforge.net al seguente link:
http://rkhunter.sourceforge.net/

Altre indicazioni le potete vedere anche a questi link:
http://www.rootkit.nl/projects/rootkit_hunter.html

Tecniche di scansione:
http://www.rootkit.nl/articles/rootkit_scanning_techniques.html

Per acchiappare e rilevare i rootkit sul protocollo Tcp/ip, potete testare anche il programma UNHide, presente sui server di sourceforge.net al seguente link:

http://sourceforge.net/projects/unhide/files/?source=recommended

Questo è un tool per l'analisi forense, quindi è in grado di rivelare processi nascosti usati sul protocollo internet dai vari rootkit.
Questo programma implementa sei(6) tecniche fondamentali per rilevare attività sospetta dovuta all'attività primaria di funzionamento dei rootkit, che abbiamo discusso già alcuni post addietro su questo blog.

Se usate un kernel Linux maggiore del 2.6, dovrete usare questi parametri di compilazione:

```
gcc -Wall -O2 --static -pthread unhide-linux*.c unhide-output.c -o
unhide-linux
gcc -Wall -O2 --static unhide_rb.c -o unhide_rb
gcc -Wall -O2 --static unhide-tcp.c unhide-tcp-fast.c unhide-output.c
-o unhide-tcp
```

Se invece avete un kernel minore del 2.6, BSD, Solaris o altro dovete usare questi parametri per la compilazione del codice:

```
gcc --static unhide-posix.c -o unhide-posix ln -s unhide unhide-posix
```

Cari bloggers, anche per oggi è tutto, fate attenzione, perché Internet è una rete amica di tutti e amica di nessuno... :-)
Concludo questo post augurandovi come sempre una buona navigazione, e siate prudenti con le Karamelle che volete assaggiare in rete... ;-))

Infezioni informatiche: I Predatori Dei Virus Perduti... ;-))

Post n°98 pubblicato il **15 Settembre 2013** da exodus1984
Carissimi bloggers, Il titolo di questo post è stato preso in prestito da un noto film per questa speciale occasione informatica...;-))
Pertanto, oggi diventeremo dei veri e propri "predatori di virus". 8-)

Infatti, in questo semplice post, voglio presentare una piccola assistenza informatica eseguita in questa ultima settimana per spiegare in modo abbastanza semplice la cattura e la rimozione dei virus presenti su un sistema Windows/Linux attraverso l'uso di una distribuzione GNU/Linux preparata appositamente per questi eventi.
Il sistema in questione è un vecchio portatile AMD-E2 con una installazione Windows 7 a 64bit.

Ci servirà per prima cosa, una distribuzione Linux preparata per affrontare situazioni di questo tipo, oggi infatti utilizzeremo la stupenda distribuzione DEFT(Digital Evidence & Forensic Toolkit) disponibile al seguente link:

http://www.deftlinux.net/

Faremo una breve analisi delle cose che ci servono, poi dovremo aprire il nostro bel terminale a riga di comando e quindi inizieremo a controllare il disco fisso del computer giunto in assistenza.
Ci serviranno almeno tre (3) directory differenti per poter eseguire questo tipo di lavoro, inizieremo con la prima creazione di tre punti di mount, quindi andate sotto la directory /mnt creata dal dvd live di Deft8:

/mnt/win directory dove monteremo il filesystem Windows
/mnt/key directory dove monteremo la penna usb
/mnt/c4   directory esplosiva per eliminare i virus trovati :-))

per creare queste tre directory, useremo il comando mkdir:

```
mkdir -p win key c4
```

```
deft8 /mnt % ls
c4  key  smb  win    (la dir smb è creata dal sistema Live al boot...)
```

Ora siamo pronti per catturare le informazioni che ci interessano.
Facciamo la lista delle partizioni del disco sotto esame usando il comando fdisk -l

```
deft8 /mnt % fdisk -l

Disk /dev/sda: 320.1 GB, 320072933376 bytes
255 testine, 63 settori/tracce, 38913 cilindri, totale 625142448 settori
Unità = settori di 1 * 512 = 512 byte
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Identificativo disco: 0xa8d6f410

Dispositivo Boot      Start    End      Blocks   Id  System
/dev/sda1   *      2048   209717247 104857600   7  HPFS/NTFS/exFAT
/dev/sda2      209717248   241174527  15728640  1b  W95 FAT32 nascosto
/dev/sda3      241174528   625108991 191967232   7  HPFS/NTFS/exFAT
/dev/sda4      625108992   625141759    16384  ef  EFI (FAT-12/16/32)
deft8 /mnt %
```

Dopo avere preso visione del disco, montiamo il dispositivo con il

comando ntfs-3g:

deft8 /mnt % ntfs-3g /dev/sda1 /mnt/win -o ro

Fate attenzione al montaggio dei dispositivi, nel primo esempio abbiamo montato il disco in sola lettura perchè durante una indagine informatica forense, bisogna trovare delle prove che abbiano dati non modificati dal collegamento al sistema operativo che deve effettuare le analisi richieste.
Per valutare il montaggio, ho portato questo esempio, se noi proviamo a scrivere qualcosa sul disco fisso incriminato, avremo questa risposta:

deft8 /mnt/win % cat > 1234.txt
bash: 1234.txt: File system in sola lettura
deft8 /mnt/win %

Montiamo adesso una key usb per depositare le informazioni che dovremo utilizzare durante la nostra analisi sul disco che verrà sottoposto a perizia.
Riprenderemo questa parte più avanti, quando dovremo valutare le informazioni di primario interesse per la nostra indagine informatica.

inserite la penna usb e date il comando :

deft8 ~ % fdisk -l

quindi rileggete l'elenco dei dispositivi:

Disk /dev/sda: 320.1 GB, 320072933376 bytes
255 testine, 63 settori/tracce, 38913 cilindri, totale 625142448 settori
Unità = settori di 1 * 512 = 512 byte
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Identificativo disco: 0xa8d6f410

Dispositivo	Boot	Start	End	Blocks	Id	System
/dev/sda1	*	2048	209717247	104857600	7	HPFS/NTFS/exFAT
/dev/sda2		209717248	241174527	15728640	1b	W95 FAT32 nascosto
/dev/sda3		241174528	625108991	191967232	7	HPFS/NTFS/exFAT
/dev/sda4		625108992	625141759	16384	ef	EFI (FAT-12/16/32)

Disk /dev/sdb: 16.0 GB, 16028794368 bytes
254 testine, 63 settori/tracce, 1956 cilindri, totale 31306239 settori
Unità = settori di 1 * 512 = 512 byte
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Identificativo disco: 0x00000000

Dispositivo	Boot	Start	End	Blocks	Id	System
/dev/sdb1	*	52	31283909	15641929	c	W95 FAT32 (LBA)

Il nuovo dispositivo inserito è stato rilevato, montiamo la nostra key e lasciamola perdere per il momento:

deft8 ~ % mount -t vfat /dev/sdb1 /mnt/key -o rw

Iniziamo la scansione e mettiamo i virus rilevati su un file di testo perchè per ora non possiamo modificare questo disco fisso:

deft8 /mnt/win % clamscan -r -i -l /mnt/key/virus.txt

Dalla capacità del disco fisso in esame e dalla quantità di dati contenuti, potremo impiegare più o meno tempo per la scansione del

nostro supporto:

```
----------- SCAN SUMMARY -----------
Known viruses: 2515445
Engine version: 0.97.8
Scanned directories: 32465
Scanned files: 178926
Infected files: 5          <---WOW!!! 5 Virus!!! :-)
Data scanned: 34489.13 MB
Data read: 46732.36 MB (ratio 0.74:1)
Time: 14025.716 sec (233 m 45 s)
```

ricordate che abbiamo due(2) dispositivi collegati in modo diverso:

```
/dev/sdb1 on /mnt/key type vfat (rw)
/dev/sda1 on /mnt/win type fuseblk (ro,nosuid,nodev,allow_other,blksize=4096)
```

adesso dovremo smontare il disco fisso che è in sola lettura(ro) e
quindi rimontarlo in scrittura (rw):

```
deft8 ~ % umount /mnt/win
deft8 /mnt % ntfs-3g /dev/sda1 /mnt/win -o rw
```

A montaggio avvenuto, ci sposteremo nella directory dove sarà presente
il sistema operativo Windows 7 e inizieremo a dare la caccia ai virus
rilevati.

```
deft8 ~ % cd /mnt/win
deft8 /mnt/win %
deft8 /mnt/win % clamscan -r -i --move=/mnt/c4 /mnt/win
```

la sintassi del programma clamscan è semplice:
-r analisi ricorsiva
-i lista virus trovati
--move=/mnt/c4 directory di quarantena
/mnt/win directory dove effettuare la scansione(disco fisso Windows)

Ricordate la creazione della directory c4 ?
Alla fine della rimozione dei files infetti, potremo decidere che cosa
farne, ovvero se tenerli in archivio per studiarli oppure eliminarli
definitivamente dal sistema.

```
----------- SCAN SUMMARY -----------
Known viruses: 2515445
Engine version: 0.97.8
Scanned directories: 32465
Scanned files: 178926
Infected files: 5      <----------ne abbiamo catturati 5... 8-)
Data scanned: 34489.13 MB
Data read: 46732.36 MB (ratio 0.74:1)
Time: 14107.720 sec (235 m 7 s)


deft8 /mnt/c4 % ls
AMV_DecDLL.dll        Win.Trojan.Agent-168241 FOUND
AMV_DecDLL.dll.001    Win.Trojan.Agent-168241 FOUND
iscsicli.exe          Win.Trojan.Expiro-1703 FOUND
ssText3d.scr          Win.Trojan.Expiro-1572 FOUND
wusa.exe              Win.Trojan.Expiro-1658 FOUND
```

Se non archiviate i files infetti per studiarli, non vi resta altro
che distruggere la directory /mnt/c4 facendola esplodere con tutto
il suo contenuto... 8-)

```
deft8 /mnt % rm -rf c4
```

Ora smontate i dispositivi che avete usato e fate ripartire il sistema windows 7 :

deft8 ~ % umount /mnt/win
deft8 ~ % umount /mnt/key

Il sistema windows 7, andrà in riparazione assistita, e vi verrà chiesto al boot del nuovo avvio, eseguite la scelta consigliata e premete INVIO. Anche qui ci vorrà un po di tempo per far ripartire il sistema, infatti la procedura che ho descritto in questo breve articolo, richiede la massima attenzione, perchè se un virus colpisce alcuni files importanti il sistema Windows 7 non parte più nemmeno con il suo programma di recupero interno, quindi potete salvare la vostra situazione se avete un backup pulito oppure un cd di installazione originale per il sistema windows 7 da dove far partire il ripristino del sistema.

NOTA IMPORTANTE !!!
La procedura che ho descritto, è molto distruttiva sia per i virus catturati, sia per i sistemi windows che vengono sottoposti a questo particolare lavoro informatico, alcuni files potrebbero essere visti come dei "falsi positivi" e messi in quarantena assieme a tutti gli altri virus che nel frattempo avrete catturato, in questo post non ho ritenuto utile allungare la sintassi di clamscan proprio per mantenere la massima semplicità anche per utenti che non conoscono troppo bene il mondo dei virus informatici e che lavorando su Windows vorrebbero eliminarli in modo definitivo.

Questo è anche il principale motivo per cui abbiamo effettuato due scansioni, la prima con il disco fisso in sola lettura che ha avuto lo scopo di rilevare quali files fossero infetti, e poi la seconda scansione in lettura/scrittura per rimuovere i files.
Con la prima scansione, abbiamo appurato che non ci sono files importanti infetti di sistema, quindi abbiamo effettuato la seconda scansione con l'intento di rimuovere tutti i virus che abbiamo trovato. :-)

Pertanto, chi fosse interessato a saperne di più, può trovare tutte le risposte che cerca in rete, potete leggervi molta documentazione dedicata e fare molte prove su sistemi operativi diversi.
Se disponete di un backup pulito e certificato, allora il mio consiglio è quello di provare questa procedura, alla fine, nel bene e nel male avrete comunque imparato qualcosa di utile in più. :-)

Cari bloggers, anche per oggi è tutto, spero che questo semplice post possa aiutarvi a mantenere puliti ed efficienti i vostri sistemi Windows/Linux. :-)

Hardware 3G: riparare il classico difetto del Traveler 3G-M :-)

Post n°99 pubblicato il **03 Ottobre 2013** da exodus1984
Carissimi bloggers, ri-eccoci di nuovo qui a spippolare questa volta alcuni tipi di hardware che potrebbero interessare alla maggior parte degli utenti smanettoni di questo piccolo blog. ;-))

Una settimana fa, mi hanno portato in riparazione due modem-router 3G e valutando il problema prima di uno e poi dell'altro, ho scoperto che tutti e due avevano un unico e solo difetto a livello hardware.

Il primo che ho smontato, aveva il particolare difetto di non accendersi mentre il secondo, rimaneva sempre acceso anche spegnendo il suo micro interruttore... 8-)

Ok!!! :-)
Oggi tratteremo i modem-router 3G di AirLive, nello specifico il modem router Traveler 3G-M 802.11b/g/n.

Ma partiamo con ordine, devo dire che questi tipi di modem-router 3G contengono una tecnologia che risale al 2009, ma si adattano molto bene a tutte le reti a cui sono collegati, infatti, portano un kernel GNU/Linux e sono rootati dal leggendario sistema BusyBox, di cui vi propino il link sottostante:

http://www.busybox.net/

Le caratteristiche tecniche di questo piccolo router 3G, le potete trovare in rete, a livello personale, ho fatto alcune configurazioni particolari e ho eseguito dei test, nelle zone a bassa copertura, si nota una netta e migliore ricezione rispetto alle classiche chiavette che i gestori nostrani ci propinano sempre...;-)))

Ma torniamo all'argomento principale di questo post, come dicevo, ho ricevuto in assistenza due modem di questo tipo, e tutti e due avevano un difetto comune: il micro interruttore interno, agganciato ad un cursore-interruttore che essendo uscito dalla sua sede, portava alla disfunzione dell'intero modulo hardware... :-(

Per prima cosa, ho aperto il vano batteria, estratto la batteria e la sim, quindi ho potuto procedere allo smontaggio vero e proprio del contenitore.

Il contenitore plastico dispone di ganci a tenuta e questi vanno forzati con un movimento circolare, altrimenti non riuscite ad aprirli e li potreste daneggiare assieme al modulo interno.
Quando fate questi lavori, assicuratevi di scaricare l'elettricità statica toccando magari un termosifone e usando un bracciale antistatico in laboratorio, ricordate che il circuito interno del Traveler 3GM è molto delicato e potete metterci meno di un secondo per distruggerlo... :-))

A questo punto, il circuito è scoperto, mettete da una parte i contenitori plastici e dall'altra il circuito modem-router, adesso dovete recuperare le parti plastiche rotte del cursore-interruttore, e cominciare ad incollare i due pezzi su una superficie piana.

Quando il cursore-interruttore sarà abbastanza asciutto, posizionatelo al suo posto in contatto diretto con il micro interruttore saldato sul circuito stampato, per favorire la messa in posizione finale, ho usato una piccolissima goccia di adesivo rapido riposizionabile in modo che rimanga fermo per il montaggio finale solo per il tempo necessario.

Per chi vuole vedere tutta la procedura, ho caricato alcune foto che possono aiutare a risolvere questo problema che è dovuto al continuo uso dell'interruttore per accendere e spegnere il modem. :-)
Il circuito interno è costruito molto bene e si presta altrettanto bene a spippolamenti avanzati che però non tratteremo in questo semplice post dedicato alla riparazione del principale difetto riscontrato da migliaia di utenti con questo tipo di modem-router 3G.

Potete cliccare su "Foto" sulla barra di navigazione di Libero qui sopra e aprire l'album "AirLive Traveler 3G-M" per vedere lo smontaggio e la riparazione di questo modem 3G.

Cari bloggers, spero che questo post possa essere di aiuto ai possessori del Traveler 3GM, afflitti da questo grave bug... ;-)))

I racconti della rete: La Leggenda del Cavaliere Informatico.

Post n°100 pubblicato il **13 Ottobre 2013** da exodus1984
Carissimi bloggers, voglio dedicare questo post ad alcuni amici che provengono dalle più sperdute lande desolate di internet... ;-)))

Pertanto, oggi vi racconterò una breve storia, curiosa e forse non troppo attendibile che riguarda appunto la vita virtuale di molti soggetti informatici strani e controversi che conosco da molto tempo... ;-))

Allora, andiamo ad iniziare:

La Leggenda del Cavaliere Informatico (CCPL BYNCND ver. 3)

"C'era una volta, tanto e tanto tempo fa, in una terra lontana lontana, un villaggio virtuale popolato da strani esseri fatti di bit il cui solo scopo era quello di impadronirsi delle informazioni riservate del Re che governava la rete internet.
Questi strani abitanti, avevano la capacità di osservare i dati in transito sulla rete e di condividerli in tempo reale con i loro propri simili.

Ci fu un tempo in cui un grande mago informatico predisse la caduta dell'impero di internet, in cui tutti i dati riservati del Re, sarebbero caduti nelle mani dei suoi nemici...
Il mago predisse la caduta dell'impero per mano di un cavaliere giunto da un altro universo informatico, e che la profezia si sarebbe avverata tra mille anni.

Intanto, nel villaggio di Kilobit, Zero e suo fratello Uno, studiavano assiduamente per poter ottenere il dottorato in smanettologia moderna.
I due fratelli erano rivali, e quello che faceva Uno, lo doveva fare anche Zero, ma erano troppo diversi per combinare qualcosa di buono senza litigare sempre tra di loro...

Non molto tempo prima, l'impero di internet era stato devastato da un massiccio attacco da parte dei predoni Virus, che avevano distrutto tutte le coltivazioni informatiche, lasciando i sudditi del Re a morire di fame, le informazioni avevano perso il loro valore nutritivo per il popolo di internet, e qualcuno ripensò alla profezia fatta dal mago tanto tempo prima...

Qualcuno, affermò che gli anni trascorsi per la profezia erano ormai alla fine, e che il popolo di internet doveva prepararsi al peggio...
Nel fragore della guerra informatica, i due fratelli avevano lottato con tutte le loro risorse hardware per poter sopravvivere, ma alla fine del conflitto si trovavano di nuovo divisi e rivali nella loro misera vita informatica.

Un triste giorno, i due fratelli vennero convocati al capezzale del loro vecchio padre morente, un ex generale delle truppe reali che aveva combattuto la guerra in prima linea ed era stato colpito da un'infezione mortale contratta durante l'ultima battaglia per la liberazione della terra di Ram contro i predoni Virus.

I due fratelli ascoltarono perplessi le ultime parole del loro vecchio genitore:

"Dovrete stare uniti per poter salvare la nostra terra fatta a finestre, voi due insieme, aprirete un varco negli universi informatici e dovrete trovare il prescelto, sarà colui che ci potrà

salvare...."

Furono le ultime parole del generale informatico, poi più nulla... :-(

I due fratelli che avevano sempre lottato tra di loro per vedere chi era il migliore, ora erano uniti, si erano uniti per aprire le porte dell'universo.

Era una notte buia e tempestosa, e i pochi pixel ancora accesi, non permettevano di distinguere bene l'orizzonte informatico dell'universo che avevano raggiunto.

"Dove siamo?" affermò Zero dopo essersi ripreso dal salto dimensionale effettuato dal portale Web della loro terra.
"Non ne ho la più pallida idea" rispose Uno.

Attesero l'alba di quel nuovo mondo informatico, ma il cielo sopra le loro teste, era sempre nero, in lontananza, riuscirono a scorgere una figura strana che si stava avvicinando a loro con grande velocità...

I due fratelli rimasero senza parole quando videro quella figura fermarsi a pochi passi da loro, un cavaliere informatico simile al salvatore narrato nelle leggende della loro terra da centinaia di anni.

Uno riprese il controllo e chiese: "Grande Cavaliere, può dirci dove ci troviamo?"
Il tempo della risposta sembrò un'eternità a Zero, la voce metallica proveniente da sotto gli scudi elettronici del cavaliere, fece tremare il terreno sotto i loro piedi:

"Questa è la terra di Terminale, e voi siete al cospetto di Hacker, signore della Riga di Comando e padrone degli universi internet paralleli"

Con una voce tremante, Zero sospirò: "Ho sempre pensato che la profezia fosse solo una leggenda... Il Cavaliere Hacker esiste veramente!!!"

Uno, che era meno soggetto alle emozioni informatiche, parlò in modo chiaro e diretto al cavaliere:
"Siamo stati inviati da un altro universo per trovare aiuto e salvare la nostra terra a finestre, i predoni Virus hanno devastato il nostro impero, e la nostra gente sta morendo di fame"

Ancora una volta la terra tremò sotto i loro piedi mentre ascoltavano la risposta del cavaliere:
"Ho visto il vostro universo in real time, ho visto la guerra che avete combattuto, il vostro mondo a finestre è minacciato non solo dai predoni Virus, ma anche dai signori della guerra informatica delle lontane terre di RootKit, per questo motivo vi aiuterò a salvare la vostra terra e la vostra gente"

Zero parlò con voce preoccupata: "Non abbiamo più energia per tornare a casa, non riusciremo più ad aprire il portale Web..."

Non fece in tempo a finire la frase che i pixel che circondavano l'oscura terra di Terminale si accesero di un verde brillante, il cavaliere lanciò alcuni comandi e il portale fu aperto, i due fratelli, avevano portato a termine la loro missione, ora, l'universo informatico da cui provenivano, sarebbe stato sempre al sicuro per gli anni a venire."

Cari bloggers, spero che questo piccolo racconto vi sia piaciuto, in fondo, ogni leggenda nasconde una verità che aspetta solo di essere scoperta, buona navigazione a tutti :-)

Truffe informatiche: conoscere per prevenire. :-)

Post n°101 pubblicato il **03 Novembre 2013** da exodus1984
Carissimi bloggers, oggi tratteremo un articolo piuttosto spinoso
dal punto di vista sia morale che personale, ma cosa sarà mai??? ;-))

Da un po di tempo a questa parte, parlando con alcuni amici di tecniche
speciali per l'intrusione(autorizzata) sui server bancari, è venuto alla
luce un problema che sembrava non risolvibile, ma andiamo con ordine.

Molte persone che mi hanno interpellato al riguardo dei propri conti
bancari online, non erano convinte della propria sicurezza usando
i servizi offerti dal proprio istituto di credito.
Queste persone, in pratica cercavano una sicurezza in più che nessuno
di noi potrebbe garantire al cento per cento...;-)))
Le persone vogliono essere al sicuro ma non conoscono i reali rischi
della gestione di un conto corrente online su internet.

Vorrei ricordare alcune semplici tecniche adatte ad evitare brutte
sorprese a chi gestisce i propri conti tramite internet:

Non rispondete alle e-mail che sembrano arrivare dal vostro istituto di
credito, andate di persona in banca e verificate l'effettiva richiesta
di dati personali.

Prima di connettervi al servizio bancario online che vi è stato offerto
controllate l'assegnazione IP del vero sito dell'istituto di credito.
Questo serve ad evitare trappole informatiche di phishing, ovvero, la
perfetta clonazione della pagina di accesso al servizio, ma con la
chiara intenzione di rubarvi i dati di accesso che tratteremo più
avanti in questo post.

Queste banali tecniche, servono a mantenere la cosiddetta "sicurezza
primaria", quella che ogni utente dovrebbe conoscere e praticare, le
persone infatti, sono solite digitare nella barra degli indirizzi il
nome del servizio bancario, ma vi posso assicurare che la creazione di
un servizio taroccato è alla portata di ogni criminale che abbia una
minima infarinatura nella creazione di una pagina web... ;-)

Infatti, potete usare per proteggervi da queste truffe un banale
servizio whois, seguito da un comando ping verso l'indirizzo letterale
che a partire da un indirizzo web(www.miabankareale.it)
vi rivela i blocchi IP assegnati legalmente al vostro servizio
bancario, ad esempio:

www.miabankareale.it <---servizio reale
127.0.0.1 <---servizio taroccato = ip non assegnato

Al nome del vostro servizio deve corrispondere un vero indirizzo numerico
assegnato, in caso di dubbio, non digitate nella barra degli indirizzi
il nome del servizio(www.miabankareale.it), ma digitate il vero indirizzo
IP reale numerico del sistema che vi rivela il comando ping.

Questo è molto utile perché gli indirizzi numerici assegnati, portano
direttamente al servizio richiesto, mentre gli indirizzi "letterali"
possono venire clonati molto facilmente, devo però affermare che a
questo proposito, anche gli indirizzi IP assegnati legalmente possono
essere usati per catturare i dati in transito, e questo senza nemmeno
perdere tempo per la creazione di una pagina web taroccata...;-))
La tecnica che viene usata in questo particolare caso, si chiama
"dirottamento informatico", dove l'intero servizio con nome e IP
assegnato legalmente, viene posto sotto il controllo diretto di
organizzazioni criminali informatiche che hanno lo scopo di controllare

direttamente le attività del servizio.

Non spaventatevi per quello che avete letto qui, se navigate la rete
potrete scoprire cose peggiori di queste...:-))

Quindi, in generale, la sicurezza può essere gestita dagli utenti
in modo molto efficiente partendo da un sistema operativo che possa
gestire solo transazioni bancarie, quindi niente download di giochi
musica,immagini, uno dei pc che avete in casa, dovrebbe essere dedicato
solo a questo tipo di uso(cosa non troppo fattibile...).

Ora passiamo alla vera analisi dei sistemi, molti servizi bancari
offrono un diverso approccio alla sicurezza sui loro sistemi, alcune
banche italiane offrono il cambiamento obbligatorio della propria
password una volta al mese, in più, vengono fornite delle piccole
chiavette dove l'utente preleva il terzo codice di accesso al servizio
che dice effettivamente al sistema che la persona che vi accede è
il legale detentore dell'account...:-)))

All'inizio di questo breve post avevo accennato ad un piccolo problema
che poi è stato risolto facendo comprendere alle persone che hanno
fatto questa richiesta che la sicurezza va ricercata non solo con i
codici di accesso bancari, ma principalmente anche con una buona
gestione del proprio computer, vale a dire che il proprio pc deve essere
mantenuto sempre in perfetto ordine, aggiornamenti di sicurezza, programmi
antivirus aggiornati, anti-spyware e nondimeno alla propria preparazione
informatica.

Molto bene, torniamo al problema che avevamo accennato in precedenza.
Molte persone preoccupate perché le loro password devono essere tutte
numeriche, si sono rese conto che nonostante il cambiamento obbligatorio
mensile e la key numerica, le loro password potessero essere prevedibili
e quindi non essere del tutto al sicuro dalle truffe informatiche.

Questo problema, in parte risolto, ha messo in luce l'effettiva
paura di queste persone, di ritrovarsi con password prevedibili e di
conseguenza usate a loro insaputa sui loro account.

Conducendo alcune ricerche numeriche, ho potuto vedere a livello
matematico che i dubbi di queste persone sull'uso delle password
sono fondati, nell'esempio successivo si vede chiaramente che la
costituzione di un archivio di questo tipo possa essere realizzata
da tutti coloro che abbiano anche un solo e minimo potere di programmare
un database di questo tipo, in questo esempio, ho ricreato in modo
fedele i due archivi che possono contenere tutte le possibili password
usate, viene evidenziato anche l'archivio che contiene i codici numerici
delle key:

```
enrico@exodus84:~/BankPass2013$ du -h *
8,0K    bankpass      3 nov 14.23 bankpass
4,0K    bankpass.c    3 nov 14.23 bankpass.c
93G     bankpass.txt  3 nov 15.01 bankpass.txt
8,0K    keypass       3 nov 14.53 keypass
4,0K    keypass.c     3 nov 14.52 keypass.c
6,1M    keypass.txt   3 nov 14.54 keypass.txt
```

Come potete notare, l'archivio delle password(bankpass.txt) è grande
93 Giga, ed è stato elaborato dal sistema in meno di trenta minuti mentre
l'archivio key(keypass.txt) è stato elaborato in circa due minuti.

Il test eseguito, ha confermato che in effetti le password numeriche
possono essere previste in modo semplice e pratico come da esempio.
Naturalmente, esistono molte altre tecniche di protezione dei servizi
bancari online, e non verranno trattate proprio per evitare che qualcuno
le possa utilizzare per derubare gli utenti di questi servizi che sono

molto utili, ma che risultano anche molto fragili se sottoposti alla legge spietata dei criminali informatici.

Cari bloggers, anche per oggi ho potuto mandare un post su questo piccolo blog, ricordate che quello che avete letto qui, potete trovarlo in rete, scritto in forme diverse ma con la stessa salsa...;-))
Come sempre, vi auguro una buona navigazione e un buon proseguimento su internet. :-)

Il Software Open Source in ambito investigativo.

Post n°102 pubblicato il **16 Novembre 2013** da exodus1984

Dunque, oggi volevo mandare un piccolo articolo che trattava la psicologia d'assalto usata dagli hacker prima di predisporre le proprie intrusioni informatiche, ma ho ritenuto opportuno scrivere una banale considerazione personale al riguardo di numerose richieste che mi sono pervenute per un evento importante che si terrà qui a Udine a fine mese.

Pertanto, per informare tutte le persone che hanno fatto questa richiesta, vi comunico che ho già dato la mia disponibilità, e se non ci sono imprevisti all' ultimo minuto, ci ritroveremo tutti quanti il 30 novembre per l' Open Source Day 2013 dalle ore 10.00 in poi.

Ci sarà la presentazione del progetto italiano D.E.F.T. e C.A.IN.E. Linux a cura del pubblico ministero della procura di udine, sostituto procuratore Dott. Andrea Gondolo, per l'introduzione del percorso forense dedicato agli strumenti Open Source, passando per l'uso delle timeline nell'analisi forense al mobile forensic praticato con gli strumenti Open source, per arrivare poi dalla OS intelligence fino al problem solving nella digital forensics sempre usando software Open Source.

Approfitto di questo piccolo post per salutare alcuni vecchi volponi di rete, se avremo abbastanza tempo, potremo discutere anche di altre questioni che vi sono piaciute, come specificato nel post precedente dedicato alle truffe informatiche sui server bancari. :-)
Sui sistemi D.E.F.T. e C.A.IN.E. Linux, avevate già letto alcuni articoli pubblicati su questo blog, e visto che i volponi saranno parecchi qui a Udine, forse potremo trovare anche altri usi per queste stupende distribuzioni Linux, che appunto nel mio campo, non servono solo per l'analisi forense... :-)))

Chiarito questo, concludo il post augurandovi una buona navigazione e naturalmente, oltre che gli amici di sempre, questo invito è da considerarsi valido anche per i bloggers di Libero che vogliono partecipare a questo evento.
Buon proseguimento a tutti voi. :-)

Computer Forensics: considerazioni personali di un evento annunciato.

Post n°103 pubblicato il **30 Novembre 2013** da exodus1984
Dunque cari bloggers, rieccoci qui a commentare la giornata di oggi sabato 30 novembre 2013 per definire l'evento di cui abbiamo parlato nel precedente post. :-)

Devo dire che tanto per iniziare bene il percorso forensics, l'aula "0" ricercata da tutti, persino da chi ci studia tutti i giorni in questa università, era la famigerata aula "L", qualcuno ha infatti affermato che la cosa era in tema con le investigazioni, e quindi i partecipanti dovevano "scoprire" dove si trovava... ;-)))
(per chi si è perso, c'erano le frecce e i cartelloni...) ;-)))

Visto che siamo arrivati un pochino in ritardo, un'amica ci ha tenuto i posti, e quindi abbiamo iniziato il percorso forensics a metà della prima conferenza prevista dal programma, ovvero l'uso delle timeline nell'analisi forense.

Nelle seguenti divulgazioni, abbiamo assistito ad ulteriori interventi riguardanti la mobile forensics, con diverse spiegazioni sull'uso ed abuso delle memorie nei telefoni cellulari, partendo dalla più comune sim telefonica e passando per le schede di espansione per tablet e cellulari, per finire con un breve ma utile accenno alle tecniche di "chip off", ovvero quando una memoria dati non può essere rimossa, e quindi bisogna dissaldare il componente e reinserirlo in una nuova architettura costruita ad hoc per estrarre i dati contenuti.

Abbiamo proseguito poi con le tecniche di base della OS Intelligence dove è stato esposto un caso specifico che era perfettamente adatto a spiegare il tema di questa conferenza, passando dalla teoria alla pratica di tutti i giorni per risolvere molte volte un caso usando solo la logica dell'analisi informativa basata sull'uso di strumenti liberi e a disposizione di tutti gli utenti di internet, le tecniche usate, incorporavano i link a cui tutti ci connettiamo ogni giorno, da Google a Facebook, passando per tutti i social network raccogliendo ed analizzando le informazioni che la ricerca si prefiggeva.

Il finale di questa giornata, si è concluso con il problem solving nella digital forensics, definito dal Dott. Bassetti "Mc-Gyver Forensics" proprio per l'uso di soluzioni immediate e utili alla situazione in corso, come ad esempio collegare una determinata periferica e riuscire ad estrarre i dati anche senza disporre di software e hardware molto costosi e magari in dotazione solo per grandi aziende o enti governativi. Cybercrime e cause civili, hanno la stessa importanza nella società in cui viviamo, e visto che un banale telefono cellulare lo possiedono quasi tutti, si può trovare una valida base di partenza per un caso di infedeltà coniugale passando per comunicazioni e SMS inviati da bande criminali ottenendo un adeguato percorso per costruire le prove a carico degli indiziati che possano essere ammesse in tribunale. :-)

Abbiamo concluso questa bella giornata in compagnia di persone che sanno fare bene il proprio lavoro, e naturalmente, un vecchio Lamer come me ha potuto aprire le porte della computer forensics a due ragazzi che volevano intraprendere e capire bene il mondo delle investigazioni informatiche, portando questo tipo di conoscenze nella loro vita.

Infatti, questo percorso è stato scelto proprio per l'interesse generato, personalmente conosco abbastanza bene le tecniche e i programmi che sono stati introdotti e spiegati durante tutte queste conferenze, anche se il mio campo è tutto il contrario, ovvero l'anti-forensics, ma non posso certo tralasciare le ottime tecniche della computer forensics con la quale condivido la mia

esistenza informatica. ;-)))
Scherzi a parte, tutti quanti ne sono usciti contenti e soddisfatti e quindi tirando le somme, molta gente ha potuto imparare cose che altrimenti non avrebbero potuto sapere, e tutto questo, dalla bocca di chi gestisce questi casi informatici per lavoro ogni giorno.

Concludendo questo breve post, posso dire che anche oggi ho imparato qualcosa, ma quello che conta di più è che la divulgazione della computer forensics possa essere sempre più praticata da tutte le persone che credono nella verità e nella giustizia (quella vera...).

Detto questo, come sempre, vi auguro una buona navigazione e una buona permanenza in rete, approfitto del post per salutare tutti gli amici che oggi non ho potuto incontrare, chiedo scusa, ma il tempo è stato tiranno, e non ho potuto essere presente dappertutto... ;-)))

Anti-Forensics: la mnemotecnica nelle truffe psicologiche informatiche.

Post n°104 pubblicato il **07 Dicembre 2013** da exodus1984
Cari bloggers, oggi parleremo di un argomento che tratta alcune tecniche avanzate che possono essere utili sia nella vita di tutti i giorni che nella psicologia d'assalto usata ormai da moltissime persone, e un tempo, terreno di battaglia degli hacker praticanti di quella che è ormai conosciutissima come "ingegneria sociale".

Premetto che questo post è forse un tantino pesante per le persone che non conoscono questa materia specifica, ma come sempre, potete trovare ulteriori indicazioni qui su internet, se magari non riuscite a comprendere bene questo articolo, che mi era stato richiesto alcune settimane fa e poi per mancanza di tempo, non ho potuto inviarlo qui sul blog.

Inizieremo a descrivere alcuni metodi banali che porteranno a capire l'evolversi delle tecniche nell'ingegneria sociale e come sfruttare queste conoscenze per migliorare la propria memoria senza però usare i metodi descritti per arrecare danno alle altre persone.
Infatti, oggi descriveremo l'uso delle tecniche di memoria usate molto spesso nella computer forensics per capire la psicologia del soggetto prima di effettuare un recupero informativo.

Partiamo con la prima descrizione:

Il soggetto che ha effettuato un crimine informatico ha delle particolari conoscenze, che potrebbero sfuggire al team che si dovrà occupare del recupero dati da un supporto sequestrato.

Il soggetto incriminato, dispone di un notevole bagaglio informatico tale da rendere davvero difficile la vita agli operatori che dovranno recuperare i dati dai supporti informatici trattati da questo soggetto.

Che cosa ci dice tutto questo?
Ci dice che prima di effettuare un recupero informativo dai sopracitati supporti magneto/ottici trattati da questo soggetto, dovremo approfondire il suo background culturale, per capire bene con quale tipo di persona dobbiamo confrontarci, e di conseguenza, che cosa possiamo aspettarci dalle protezioni inserite sui supporti da questo soggetto informatico.

Nella psicologia d'assalto, esistono diverse tecniche che possono essere utilizzate dal soggetto per confondere e prevenire la scoperta di prove a suo carico, e pertanto, si deve procedere ad una analisi approfondita della mente del criminale informatico.

Computer forensics, anti-forensics e psicologia d'assalto applicata sono pertanto da ritenersi una cosa sola, sia nell'ambito di un soggetto informatico criminale che nel recupero dati da supporti provenienti da una mente preparata e che giustamente, non possono essere ignorati dagli investigatori informatici ne dal team che dovrà trovare le prove legate a questi supporti.

L'arte di aiutare la memoria, viene praticata ad alto livello da numerosi soggetti informatici e, anche se ignorata, pure da tutte le persone comuni tutti i giorni.
Pertanto, la mnemotecnica, viene descritta come l'arte di addestrare la propria memoria con procedimenti artificiali adatti a creare un soggetto informatico dalle capacità superiori, in grado di dare filo da torcere a intere squadre di investigatori informatici.

La mnemotecnica, viene usata fino dall'alba dei tempi, infatti gli esseri umani, sfruttano da sempre tutti i sistemi ingegnosi per cacciare, per imparare e per poter ricordare quando poi un evento simile si dovesse ri-presentare.
Tutti noi lo facciamo inconsciamente, senza rendercene conto, proprio perché tutto quello che abbiamo assimilato da eventi precedenti, ci permette di essere competitivi e di sopravvivere alla società.

I sistemi mnemotecnici, possono essere molto avanzati, e per questo motivo non tutte le persone possono assorbire, ricordare e riutilizzare quello che hanno imparato, non tutti i soggetti addestrati possono avere lo stesso profitto nel ricordare un evento, ricostruirlo o descriverlo nei più piccoli particolari quando gli viene richiesto.

Nell'addestramento di un soggetto, devo dire che i migliori procedimenti mnemotecnici sono quasi sempre quelli che il soggetto può trovare da solo, e aiutato da uno specialista di questo particolare settore, si può ottenere un brillante esempio per aiutare la descrizione del tipo di persona che ha commesso il crimine informatico, decidendo poi la strada da seguire per il recupero di particolari supporti informatici ottenendo quello che viene comunemente chiamato "profilo psicologico".

Ma andiamo oltre, l'investigatore informatico deve conoscere molto bene il background del criminale informatico, per cui, valutiamo alcune tecniche usate nella mnemotecnica artificiale:

1) il criminale informatico dispone di un'agenda mentale completa, in grado di operare avanzatissime tecniche psicologiche di anti-forensics.

2) le tecniche del criminale informatico, sono applicate in modo paranoico secondo il suo addestramento e il grado di preparazione raggiunto dal soggetto stesso su tutti i suoi supporti digitali.

3) sistemi di collegamento, schemi connettivi avanzati, ne fanno un elemento non comprensibile alla mente di un investigatore informatico che non conosce queste tecniche e non le applica al caso trattato.

La nostra risposta a un caso di questo tipo, è che bisogna preparare il team che si occuperà della computer forensics sui supporti digitali di questo soggetto in modo adeguato e valido, senza mai sottovalutare il potenziale effettivo di un criminale informatico addestrato ad usare queste tecniche.

Devo dire che molte volte, questo non succede, perché gli investigatori informatici si sentono sempre "superiori" ai criminali digitali solo perchè fanno questo lavoro per professione o peggio ancora, si sentono importanti perché magari lavorano per un'agenzia governativa.
E poi vengono raggirati da persone comuni e cadono come pere...;-))

L'addestramento del team che dovrà condurre l'indagine informatica forense, dovrà pertanto essere predisposto per fronteggiare eventi di questo tipo, senza sottovalutare mai e poi mai la vera preparazione del criminale informatico.

Molte volte la mnemotecnica artificiale, viene presa come "telepatia" affermata, ma in realtà, questo non è vero, perché la mnemotecnica usa un codice predisposto o una frase specifica per scoprire il colore di una camicia, il colore dei capelli dato ad indovinare al classico "telepata" nelle fiere da baraccone...;-)))
Tutto questo, stupisce e muove l'ammirazione delle persone presenti ad una dimostrazione di questo tipo, ma l'uso che ne viene fatto nell'anti-forensics è da tenere in seria considerazione durante una indagine informatica che riveli la presenza di queste tecniche applicate ai supporti digitali, e in grado di depistare perfettamente gli

investigatori non preparati.

Cari bloggers, per oggi credo che possa bastare, spero che questo post risulti abbastanza comprensibile per tutti, ho cercato di spiegare in modo semplice uno degli aspetti della memoria hacker passando dalla computer forensics all'anti-forensics, ma in ogni caso ho fornito la base di ricerca ad alcuni amici che avevano fatto questa richiesta alcune settimane fa.
Come sempre vi auguro una buona navigazione, ricordandovi di fare molta attenzione durante le vostre indagini informatiche, perché a volte, i più furbi non siamo noi... :-)

Computer Forensics: la DarkNet Intelligence.

Post n°105 pubblicato il **01 Gennaio 2014** da exodus1984
Carissimi bloggers, augurandovi un buon inizio per l'anno nuovo, oggi parleremo di sicurezza di base e di indagini particolari, dedicate al mondo sommerso, ovvero la faccia oscura di internet...;-)))

il primo post di questo 2014 è dedicato ad un argomento che ha avuto una grandissima diffusione all'interno della nostra rete privata, per cui, viste le particolari insistenze di alcuni amici, è stata presa la decisione di pubblicare su questo piccolo blog un resoconto semplificato di come si può usare un comune sistema operativo per renderlo adeguato ad eseguire indagini particolari operando all'interno delle reti oscure presenti qui su internet.

Devo dire che molte sono state le domande poste, e ad ognuna di esse è stata data una risposta reale, quello che andremo a fare con il nostro sistema operativo, non sarà pertanto nulla di illegale, anche se molta gente pensa che le reti cifrate e anonime nascondano soltanto criminali informatici incalliti che vendono i loro servizi al miglior offerente, nel nostro caso invece, tutto questo ci servirà per raccogliere informazioni particolari e creare un rapporto di analisi che riguarda la cosiddetta "DarknetIntelligence".

Ma che cosa significa questa strana parola?
Provate a cercarla su Google: DarknetIntelligence ;-)))

Prima di tutto dobbiamo fare riferimento alla Computer Forensics, dalla quale scaturiscono le innumerevoli tecniche e tecnologie sviluppate per l'Anti-Forensics usata appunto all'interno delle DarkNet.
Dark Net, definizione poco pregevole di "Mercato Nero", alcune recenti definizioni, dicono che le DarkNet sono un pericoloso mercato nero in cui criminali, terroristi, hacker, hanno creato questa nuova realtà virtuale dove poter comprare e vendere qualsiasi cosa.

Come avevamo appurato in una ricerca fatta un po di tempo fa e pubblicata su questo blog, tutto questo, è reale, ma quello che serve a noi non è sapere come usare una rete di questo tipo, ma si presume che gli utenti abbiano almeno una discreta base informatica prima di eseguire programmi che sbandierano sicurezza e anonimato senza fornire una garanzia di quello che stanno dando ai clienti sprovveduti che magari vogliono acquistare della droga su questi siti particolari e pensano che nessuno ne potrà sapere mai nulla perché sono "anonimi"...:-)))

La Darknet Intelligence, mira a raccogliere informazioni attraverso agenti software infiltrati attraverso i vari nodi di scambio cifrati presenti durante una connessione "anonima".

Questi agenti software, hanno il semplice scopo di catturare, cifrare e spedire i dati raccolti ad un particolare sito web creato proprio sulla rete anonima sotto controllo al fine di poter ottenere una valida analisi dei dati raccolti per fornire prove robuste e affidabili per poter incriminare chi vende armi, droga e pedo pornografia online.

Questo concetto, non risulta però valido se usato dalla controparte ovvero la AntiDarkNet-Intelligence, praticata da elementi addestrati da qualche agenzia governativa che magari ha degli interessi particolari su questo tipo di rete, non sono da meno i gruppi terroristici che scambiano informazioni e materiale particolare, a questo proposito, si può osservare un aumento delle capacità tecnologiche applicate per ottenere una cifratura più robusta usando nodi preparati appositamente per questo tipo di attività.

La raccolta informativa, implica anche una preparazione particolare del sistema operativo che si dovrà usare per effettuare le investigazioni informatiche all'interno del complesso sistema DarkNet presente oggi.

A questo proposito, useremo il sistema Tor non per commettere azioni illegali ma bensì per creare un client di indagine dal quale poter effettuare una analisi informativa che ci permetta di ottenere un buon risultato finale.

Per portare un banale esempio reale, è stata utilizzata una distribuzione GNU/Linux molto conosciuta, la leggendaria Debian (Wheezy 7.2).
La preparazione di questa distro Linux, è quella riportata su tutti i principali manuali online di sicurezza informatica, ma qui ne vedremo solo una parte, proprio perché la gestione di un client completo e funzionante richiede una buona preparazione in materia di porte, servizi offerti, demoni in ascolto, etc.etc... :-)

Non voglio addentrarmi a spiegare tutte queste cose per non appesantire troppo gli utenti che leggono questo semplice post, e non riescono a comprendere bene i protocolli usati, le cifrature e quant'altro, per cui passiamo al sodo valutando i primi risultati che possiamo ottenere preparando il nostro client per la prima analisi informativa su una oscura rete anonima:

Disabilitare le porte internet per i servizi RPC che non ci servono:
da root =>> update-rc.d rpcbind disable

I seguenti servizi potete fermarli anche da gestione servizi(grafica) dipende da che cosa avete installato sulla vostra Debian, ma in genere leggetevi i manuali dei servizi che avete in esecuzione per fermarli sospenderli o riavviarli a vostro piacimento.

exim4
rpcbind
rsync
rsyslog
nfs-common

Avremo così ripulito e chiuso ulteriori porte che non ci servono sul nostro sistema.
Questi servizi vanno disabilitati solo se non sono realmente necessari per la connessione a internet o per il loro specifico uso sul sistema.

Ecco un output di quello che potete ottenere:

```
enrico@exodus84:~$ netstat -na | grep tcp

tcp        0      0 127.0.0.1:631           0.0.0.0:*         LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN


root@exodus84:/home/ghost# netstat -nap | grep tcp

tcp        0      0 127.0.0.1:631           0.0.0.0:*         LISTEN
3270/cupsd
tcp6       0      0 ::1:631                 :::*                    LISTEN
3270/cupsd
```

Eliminiamo anche il demone schedulatore di stampa cupsd (Internet Printing Protocol, version 2.1)e potremo ottenere questo risultato sulle porte disponibili del nostro client internet:

```
enrico@exodus84:~$ netstat -na | grep tcp
enrico@exodus84:~$
enrico@exodus84:~$ netstat -na | grep udp
enrico@exodus84:~$

root@exodus84:/home/ghost# netstat -nap | grep tcp
root@exodus84:/home/ghost#
root@exodus84:/home/ghost# netstat -nap | grep udp
root@exodus84:/home/ghost#
```

Avvio di Tor in ascolto:

```
enrico@exodus84:~$ netstat -na | grep tcp
tcp        0      0 127.0.0.1:9050          0.0.0.0:*         LISTEN
enrico@exodus84:~$ netstat -na | grep udp
enrico@exodus84:~$
```

Tor, verrà eseguito sul sistema senza l'uso di Privoxy, la definizione di questo proxy web, serve per aumentare la sicurezza con l'uso di Tor, ma nel nostro caso, ne faremo a meno per questa volta.

Visto che vogliamo fare delle ricerche informative per una DarkNet Intelligence Agency, dovremo raccogliere molte informazioni e poi collegarle tra di loro.

Rifiutando Privoxy, il nostro sistema d'assalto Debian per le Darknet eviterà di filtrare i contenuti che accresceranno i nostri dati per l'analisi informatica da eseguire, e questo, ci fornirà numerose informazioni primarie.

Quindi la preparazione di un sistema completo, si potrà ottenere con un sistema Debian di base e poi lavorando alla chiusura delle porte che risultino ancora visibili ad una scansione di rete.
A questo, dovrà seguire una adeguata compilazione del kernel nella vostra distribuzione, inserendoci tutti i vostri moduli d'assalto per preparare il sistema al lavoro che dovrà svolgere.

Studiate bene il manuale di Tor, per capire come e dove potete mettere le mani per ottenere quello che vi serve, visto che dovremo lavorare su una rete anonima, avremo il nostro bel da fare per catturare tutte le informazioni richieste, metodo difficoltoso ma possibile. :-)

Gli applicativi client come Firefox, possono usare la rete Tor collegandosi all'interfaccia proxy socks locale fornita dall'istanza di Tor.
Se l'applicazione stessa non supporta SOCKS, è possibile usare un client socks come torsocks.

Su Firefox, una volta generata la connessione alla rete Tor, dovrete impostare il browser perchè possa usare SOCKS4/5, altrimenti non potrete navigare all'interno della rete anonima.
per impostare Firefox dovete andare sul menù:

Modifica -> Preferenze -> Avanzate -> Rete ->
Determina come Firefox si connette ad Internet -> Impostazioni ->
Configurazione manuale dei proxy -> Host SOCKS:

Impostare Host SOCKS a: 127.0.0.1 porta 9050
e quindi cliccare su OK.
Da questo momento sarete "TORificati" e pronti per la vostra indagine informativa nei bassifondi di Internet. :-)

Cari bloggers, anche per oggi è tutto, ho cercato di accontentare un po tutti quanti con questo semplice post, come sempre se non riuscite

a comprendere alcuni significati di quello che ho scritto, potete trovare tutte queste informazioni in rete, che possono spiegarvi bene e forse in modo più semplice tutto quello che volevo esprimere qui.

Buon 2014 a tutti, investigatori informatici e hacker compresi :-)

Libertà digitale: Tecniche di base per la protezione dei dati personali.

Post n°106 pubblicato il **25 Gennaio 2014** da exodus1984
Cari bloggers, rieccoci finalmente qui su questo piccolo blog a trattare argomenti strani... :-)))

Va bene, torniamo seri per almeno due minuti e anche oggi potremo discutere di un argomento importante che ci riguarda tutti, nessuno escluso... ;-))

Oggi voglio parlare di sicurezza, ma questo tipo di sicurezza si dovrà applicare al proprio modo di lavorare su internet, per capirci meglio, oggi impareremo a difendere la privacy dei nostri file da molteplici attacchi portati a termine su computer e reti private da parte di curiosoni di varia natura e con interessi particolari, si può pertanto capire che la difesa delle informazioni che riteniamo importanti, sono oggetto di desiderio da parte di persone particolari ma soprattutto di controlli effettuati dai vari governi senza che le persone comuni ne siano al corrente... :-)))

Dovete sapere che esistono migliaia di assalti possibili e altrettante nuove tecniche di intrusione informatica che vengono fatte ogni giorno ai danni di ignari utenti di internet da parte di elementi che vogliono avere il controllo non solo su quello che andate a fare in rete, ma anche controllare il contenuto dei vostri documenti personali per sapere come la pensate e se la pensate in modo diverso per potervi "iscrivere" nelle loro liste dedicate alle persone che meritano di essere "osservate"... :-))

Fino a questo punto, penso che tutti voi sappiate che internet non è certo un bel posto, ma proseguiamo un passo alla volta, come diceva un tempo qualcuno: "la fuori è tutto un Far West...", quindi è bene ricordare soprattutto ai nuovi arrivati qui in rete, che la connessione internet da un accesso bidirezionale, e questo comporta che il vostro nuovo e fiammante computer, sarà esposto sempre a qualsiasi attacco perpetrato da persone diverse, per cui, molti di voi si staranno chiedendo: "ma io non ho nulla da nascondere...", oppure:"io non ho una azienda e quindi non possiedo segreti..." :-)

Allora vi posso dire che tutto questo, non ha la minima importanza per chi vuole porvi sotto il suo controllo, al giorno d'oggi, non serve essere un Boss della malavita per essere posti sotto il controllo di qualcuno, ma basta solo avere una connessione alla rete internet per venire "catturati", e, anche se avrete un'anima candida e pulita(come la mia???:-)), qualcuno, vorrà sempre sapere ugualmente tutto quello che vi può riguardare... :-))

Molto bene, adesso però passiamo ai fatti e come sempre, andremo a vedere come ci si può difendere da questi attacchi che ormai non mirano più a bucare sistemi per "divertimento" nel caso di hacker, ma per pura necessità di controllo da parte di persone che si ritengono al di sopra di tutto e di tutti voi solo perché lavorano per una qualunque agenzia(sorveglianza privata, sorveglianza governativa).

Visto ed appurato che la libertà individuale è solo un'utopia, quello che dovremo fare è molto semplice:

1) Non possiamo evitare questi assalti, per cui impariamo a prendere conoscenza del problema per studiare le contromisure adeguate alla situazione corrente.

2) Dato che non possiamo evitare questi assalti, impariamo a rendere quantomeno difficoltoso e impossibile il lavoro di questi curiosoni informatici.

3) Trovare le soluzioni più adeguate al sistema operativo in uso e mettere in atto una valida contro-offensiva per rendere inutili i tentativi di questi estranei a leggere le informazioni che ritenete riservate.

Devo premettere che però gli utenti "normali", non possiedono macchine con una potenza di calcolo abbastanza adeguata per preservare con delle semplici cifrature i loro dati informatici, esistono centri di calcolo che vengono costruiti e usati solo per effettuare questo tipo di lavoro e decifrare anche codice molto robusto.

Allora come ovviare a questo problema?
In rete, potete trovare migliaia di programmi per cifrare i vostri file, questa, è solo una banale tecnica per dare una piccola protezione informatica al vostro lavoro, però non può bastare a proteggerlo dai centri di calcolo che lavorano ogni giorno per scoprire quello che avete criptato nei vostri documenti personali riservati... :-)

Possiamo utilizzare in questo caso, una tecnica molto antica, ovvero creare un programma che possa usare almeno una trentina di algoritmi di cifratura diversa creati appositamente per difendere solo il nostro lavoro personale mixando le sequenze criptate assieme alla delocalizzazione del lavoro criptato, depositando parti del nostro file sui server di tutto il mondo, e mantenendo una chiave simmetrica a mappa globale delocalizzata che aprirà il vostro archivio riservato dove e come vorrete voi, rendendo anche la stessa chiave usata per proteggere i vostri dati, introvabile.

Partiamo dalla creazione della chiave di apertura, il metodo più semplice per crearne una è quello di inserire in una directory molti file spazzatura, ovvero file eseguibili, immagini, testo, tutto materiale considerato "inutile", quindi quando avrete raggiunto la dimensione di 4,7 Gb, trasformate la directory spazzatura in un file .ISO masterizzabile da un comune DVDwriter, a questo punto però non dovrete masterizzare questa immagine.iso, ma dovrete dividerla, ovvero fate a "fette" questa immagine criptata e solo allora potrete scrivere ogni parte su un supporto diverso, tenendo presente la sequenza numerica di ricostruzione della chiave.

Alla fine di questo breve lavoro, avrete una chiave simmetrica condivisa con più persone di vostra fiducia, in parole povere, tutti potranno avere la possibilità di aprire l'archivio riservato, ma nessuno potrà mai farlo se gli altri membri non concedono l'uso della parte di chiave in loro possesso, finché la chiave non verrà ricostruita l'archivio non potrà essere aperto, ma anche disponendo di tutti i pezzi della chiave, senza la mappa di localizzazione dell'archivio cifrato non sarà possibile l'utilizzo della stessa chiave rigenerata.

Questo, è solo un banale esempio di quello che si può creare per proteggere le proprie informazioni dagli sguardi indiscreti di chi vuole controllare la vostra vita informatica. :-)
Esistono migliaia di gabole informatiche che si possono utilizzare per proteggere in modo abbastanza robusto le nostre informazioni personali, per questo motivo l'Anti-Forensics può insegnare molte cose alle persone che vogliono difendere la loro libertà su internet senza essere considerati "delinquenti" solo perché hanno avuto l'ardire di nascondere delle informazioni cifrate in un archivio condiviso a livello globale.

Bisogna ricordare a tutti che solo voi potete decidere della vostra libertà di pensiero sulla rete, ma posso affermare che non sempre si può avere tutto, e quindi bisogna sapersi accontentare, tenendo alla larga certi curiosoni dai nostri file riservati con ogni mezzo informatico disponibile. ;-))

Questo piccolo post è scaturito da una discussione sulla sicurezza informatica a livello personale che ha avuto inizio su una Darknet esterna alla rete Tor, dalla quale sono stati portati alcuni esempi validi e confermati a livello di programmazione che dimostrano la validità di questa tecnologia applicata all'Anti-Forensics.

L'uso del calcolo distribuito sfruttando i server dei nodi cifrati e nascosti, permette al singolo utente di avere la potenza di calcolo che il suo singolo computer non potrebbe mai ottenere per la costruzione di un archivio criptato abbastanza robusto da resistere agli assalti informatici più impegnativi.
Naturalmente, la rete deve essere davvero anonima per poterlo fare, e questo perché ormai la rete Tor è conosciuta da tutti e non ci si può più fare affidamento, stanno infatti per essere sviluppate e costruite nuove tecnologie di rete, che permetteranno di ampliare questo tipo di rete anonima rendendola certamente migliore, anche se ormai, ha perso per così dire, "l'anonimato", non nel senso della cifratura...:-)

Cari bloggers, anche per oggi sono riuscito a scrivere un post su questo blog, purtroppo il tempo è tiranno, e non mi è stato possibile inviare prima questo articolo, infatti, volevo parlare di un altro argomento, ma provvederò in seguito a farlo, tempo permettendo. :-)
Buona navigazione a tutti voi e buon divertimento su qualsiasi rete anonima e non che possiate frequentare. :-)

Recupero installazioni e fermi macchina: un RATTO per amico... ;-))

Post n°107 pubblicato il **23 Febbraio 2014** da exodus1984
Cari bloggers, dopo estenuanti fatiche informatiche posso finalmente tornare su questo piccolo blog per raccontarvi gli ultimi avvenimenti in merito ad alcune ricerche concluse nelle ultime settimane.

In questi ultimi tempi, ho avuto a che vedere con diverse situazioni informatiche di vario tipo, e per le quali ho dovuto ricorrere ad un uso estremo della "forza informatica"..., come giustamente diceva qualcuno, "che la forza (informatica...) sia con te". ;-))
Azz... ;-) ...Il lato Oscuro della Forza... ;-)))

Inizierò quindi a chiarire alcuni punti critici che mi hanno fatto lavorare più del previsto, portandomi ai limiti dell'ignoto... :-))
Vorrei dire alle persone che mi conoscono che le gatte informatiche da pelare, non dovrebbero arrivare sempre qui da me, ma ritengo che ogni persona abbia le capacità per poter risolvere il 90 percento dei problemi informatici che incontra sulla rete...;-)

Imparare come si scrive un programma, uno script bash, o qualche altro tipo di uovo pasquale per i navigatori del web, credo che sia davvero alla portata di tutti, ok, adesso che ho scaricato lo stress informatico posso passare ad elencare alcuni semplici consigli per chi non ha presente la banalità della base di un corretto approccio per mantenere in sicurezza il proprio computer e i propri dati.

Posso elencare alcuni punti seguiti alla lettera da quasi tutti gli utenti che arrivano qui su internet per la prima volta, questo è quello che ho potuto valutare dalle centinaia di installazioni per sistemi Windows e Linux, in pratica, il sistema operativo usato dalla maggioranza degli utenti che hanno avuto più fermi macchina dovuti ad una scarsa informazione di base:

1) l'utente compra il pc portatile/fisso, una connessione mobile o fissa e si "butta" sulla rete senza pensarci un attimo...

2) l'utente scarica programmi, naviga siti web non affidabili perché "consigliati" dagli amici...

3) l'utente installa uno,due,tre antivirus, e senza fare nessun tipo di configurazione, crede che il proprio sistema sia al sicuro...

4) l'utente impara a conoscere i virus, i rootkit, ma l'attrazione verso i social network dove farsi la lista degli amici è davvero troppo allettante...

5) un brutto giorno, l'utente si rende conto che i suoi dati sono la nuova identità informatica di altre persone e comincia a vagare come uno zombie alla ricerca della propria identità informatica perduta...

Adesso vi chiederete perché ho fatto tutta questa trafila, ma se qualcuno di voi ama leggere storie interessanti, ricorderà di certo un capitolo interessante di una storia (informatica) infinita... ;-)

Dal libro della Genesi:

E Dio creò gli Utenti.
E Dio vide che questo era Buono.
E Dio li benedisse, dicendo: "crescete e moltiplicatevi su Internet nelle reti locali e governative".

Cari bloggers e cari amici, nessuno può negare che tutto questo non sia vero, infatti nonostante quello che ho sempre insegnato ai miei utenti su come basare un minimo di attenzione per avere non la sicurezza informatica vera e propria(utopia...) ma un minimo di considerazione su come ci si dovrebbe comportare in rete e su come fare una configurazione di base ai propri sistemi, ebbene, nonostante tutto quello che ho fatto per preservare quel minimo di sicurezza che ogni utente dovrebbe poter mantenere, nelle ultime settimane sono stato praticamente sommerso dalle richieste disperate di utenti a cui il pc non funzionava più, alcuni utenti, sono persino riusciti a piallare intere distribuzioni GNU/Linux, solo perché volevano vedere il sistema installato sulle loro macchine.

Molte persone mi chiedono come riesco a superare sempre tutti questi disastri informatici, e purtroppo devo dire che a volte, sono costretto a rifiutare il mio aiuto a parecchie persone, per mancanza di tempo e per la scarsa attitudine di certi utenti che non vogliono imparare e vogliono che a risolvere i loro problemi, sia qualcun altro. ;-))) Sopravvivere agli utenti non è certo facile, anche perché le persone pensano in questo modo: "tu sai come fare, quindi risolvi i problemi".

Ho imparato molte cose, e continuo ad imparare ogni giorno, quindi se posso farlo io, penso che possano farlo benissimo anche gli altri. Ma tornando agli utenti, quello che posso dire è che imparando ogni giorno qualcosa, ho salvato i vostri sistemi con le conoscenze che ho acquisito nel corso della mia esistenza informatica, e che mi hanno permesso di sviluppare negli anni una distribuzione GNU/Linux personale in grado di risolvere quasi tutti i guai che gli utenti fanno ai loro sistemi Windows/Linux.

Non ho mai menzionato l'uso di una particolare distribuzione GNU/Linux per il recupero dei fermi macchina, ma su questo blog, ne abbiamo presentate parecchie che possono essere usate da tutti per il recupero dei propri sistemi operativi, basta solo guardare cosa offre il panorama informatico e valutare quello che realmente ci serve.

Per questo motivo, alcuni utenti hanno potuto assistere di persona al recupero dei loro sistemi, usando una distribuzione particolare creata e basata sulla Debian (www.debian.org), che oltre a fare cose banali come ripulire i pc da virus e rootkit, incorpora anche tutto quello che ho imparato e fatto negli ultimi venti(20) anni nel settore informatico.

Per la gioia degli amici, inserisco nella sezione "Foto" di questo blog alcune schermate catturate appositamente dalla nuova versione del sistema RATTO, già evidenziato in precedenza per il suo uso sulla rete Tor e per le spiccate doti forensics/anti-forensics e nella Darknet Intelligence avanzata.
Ma chi mi conosce bene, sa che non mi sono fermato qui, ma che ho proseguito il mio cammino per ottenere il sistema operativo che ho sempre desiderato, infatti il sistema RATTO, altro non è che una implementazione particolare di un antico progetto informatico del lontano 1999, basato su kernel BSD nelle architetture i386, e poi successivamente trasformato in quello che poche persone hanno potuto usare e conoscere, il leggendario kernel "Talpix2" nella sua implementazione più avanzata usando pacchetti Linux/BSD per la creazione di un sistema d'assalto avanzato (per l'epoca...1999) .

Non voglio riaprire vecchie ferite informatiche, ma questi erano gli anni in cui le guerre informatiche erano all'ordine del giorno, e il kernel Talpix2 era stato costruito per montare moduli per l'assalto informatico come il TcpKombat, e il [Guardian] per la difesa e la localizzazione delle reti nemiche.

Sempre in questi anni, faceva la sua comparsa il progetto "Lepus", una

delle prime vere implementazioni di psicologia digitale applicata ad un modulo del kernel in grado di sfuggire agli inseguimenti informatici.

Il nome deriva dalla mitologia greca, in cui Orione(il cacciatore), cerca la preda (la lepre) , ma non si accorge che la lepre è astutamente accovacciata ai suoi piedi e pertanto invisibile ai suoi occhi.

Nella mitologia moderna, questo fà riferimento all'hacker(il cacciatore) che cerca la sua preda in rete, in questo caso un server da bucare, ma non si accorge che il server(la moderna lepre elettronica), finge astutamente di cadere sotto i suoi colpi, mentre in realtà è il cacciatore che diventa preda... :-)))

Cari bloggers, anche per oggi è tutto, spero di non avervi annoiato troppo cavalcando il viale dei ricordi, per gli amici: il sistema RATTO che avete visto, non è in vendita, ma penso di potervi accontentare con una versione più leggera di quella che uso sempre per rimettervi in funzione i sistemi che distruggete... ;-)))

Buona navigazione a tutti e buon divertimento :-)

Etica Hacker: come sopravvivere alla rete...;-))

Post n°108 pubblicato il **23 Marzo 2014** da exodus1984
Cari bloggers, oggi apro questo piccolo post per rendere omaggio agli smanettoni più sfrenati, in parole povere, quelli che sono in grado di ottenere una cosa diversa dalla costruzione pratica di qualsiasi oggetto... :-)

Facciamo un breve esempio: se dobbiamo sopravvivere, bisogna sapersi arrangiare con quello che l'ambiente circostante ci fornisce, e quindi dobbiamo adattarci, adattare e modificare tutto quello che ci può servire per questo scopo.

Negli anni, ho potuto imparare molte cose, ma quello che ho potuto fare, è stato l'inizio della creazione di migliaia di progetti strani che poi ho usato moltissime volte sulle varie reti nazionali ed estere che mi hanno permesso di comprendere a fondo il campo dell'informazione e le informazioni stesse.

Come dicevo prima, se vogliamo sopravvivere alle informazioni, dobbiamo prima di tutto comprenderle e quindi poi riutilizzarle per i nostri scopi personali.
Le informazioni in un'epoca come la nostra, sono la merce di scambio preferita per poter ottenere tutto quello che ci serve per produrre sistemi di vario tipo, adeguati al lavoro che dovremo svolgere per ottenere ancora più informazioni...;-))

Tutto questo, calza a pennello per gli Hacker, ma il loro concetto di sopravvivenza, va molto oltre all'uso ed abuso delle varie tecnologie informatiche e non, e questo ci porta ad una considerazione abbastanza classica: l'Hacker gioca con tutto quello con cui viene in contatto, ma semplicemente piace perché le motivazioni sono spesso incentrate sulla soddisfazione personale raggiunta nel costruire una gabola di rete, violare reti e sistemi protetti, o magari per il semplice motivo che anima la ricerca e la mente di questi soggetti.

Su questo blog, sono stati esposti diversi concetti riguardanti le menti Hacker, ma la sopravvivenza in rete è generalmente un valido motivo per approfondire i vari concetti di libertà e indipendenza ricercati da moltissimi smanettoni italiani ed esteri.

I vari Governi, ci mettono sempre le zampe in mezzo, e ai poveri Hacker, non rimane ne libertà ne indipendenza... ;-)))
Ma torniamo al problema della sopravvivenza, quanti di voi sanno che un Hacker preparato può risolvere in pochi secondi problemi di vario tipo, non necessariamente incentrati al campo informatico?

Il termine "Hacker" significa "il tutto", ma quanti possono davvero dire di sapere e conoscere tutto?
Per potersi definire Hacker, bisognerebbe quindi sapere tutto, cosa per il momento non fattibile per la limitata capacità cerebrale raggiunta al nostro attuale stadio evolutivo.

Quindi, l'evoluzione degli Hacker è sempre basata sul "saperne di più" e quindi la sfida viene sempre accettata al solo scopo di raggiungere l'informazione e quindi un nuovo passo evolutivo che porterà questa particolare specie autoctona di smanettoni un gradino più in alto e più vicino ad essere una cosa sola con "il tutto".

Nel 1991 John Gilmore immaginava come potesse essere una società costruita sulle regole Hacker:

Cosa succederebbe se costruissimo una società in cui le informazioni non venissero controllate?

Come sarebbe una società in cui non devi lasciare il tuo numero di carta di credito per comprare qualcosa?

Come sarebbe una società in cui si possa avere una patente di guida senza lasciare il proprio nome?

Come sarebbe una società in cui si possa inviare e ricevere messaggi senza rilevare la propria posizione fisica ai controllori governativi?

Oggi, a più di venti anni di distanza temporale, possiamo dare una sola risposta a tutti questi interrogativi:

la rete Tor... :-))

Sulla rete Tor si usano Bitcoins, Dogecoin, etc... :-))

Per le patenti di guida, passaporti e altre identità, idem... :-))

Servizi criptati e anonymail router... :-))

Tutto questo, ci mostra quanto il pensiero e il desiderio di fare e ottenere il risultato cercato, possa contribuire a realizzare l'idea di partenza al suo termine ultimo, ovvero la realtà.
Devo dire che negli anni, ho visto in modo diretto lo sviluppo di varie correnti di pensiero informatico, e il tutto si è sempre tradotto in una nuova e strabiliante tecnologia, in grado di catturare tutte le aspettative delle persone, anche quelle di un vecchio tapiro di rete come me... ;-)))
E poi vedo le persone che conosco tutte con l'ultimo smartphone uscito sul mercato grande come una piastrella, e che non ne possono fare a meno, mentre io vivo benissimo con il mio vecchio cellulare dell'età della pietra(informatica...;-)))

Il pensiero di avere tutta questa tecnologia, è spaventoso, ma come affermavo in precedenza, il saggio è chi sa spippolare, non chi può comprare le più recenti tecnologie... :-)

Tornando al discorso della sopravvivenza, posso dire che anche io me la sono cavata discretamente bene in passato, ma anche al giorno d'oggi non mi lamento di come e di cosa riesco a fare per poter sopravvivere in questo mondo ormai guidato da una corrente iper tecnologica che proietta tutti quanti noi avanti nel futuro ma che a volte ci fa perdere il contatto con il nostro passato.

Sono sopravvissuto ricordando tutto quello che ho imparato, tutto quello che ho costruito, tutto quello che ho fatto, per chi vuole capire il vero significato di questo piccolo post, inserisco come sempre alcune immagini nella sezione "Foto" di questo blog per aiutarvi a comprendere il mio antico mondo informatico, dove esistevano reti strane e incredibili basate su antichi componenti elettronici, come direbbe qualcuno: "Dove nessun uomo è mai giunto prima..." ;-)))

Con la crescita delle tracce elettroniche che lasciamo dietro di noi ogni giorno, la sopravvivenza in rete diviene una cosa ricercata da tutti quelli che credono fermamente nell'etica Hacker, ovvero la ricerca della propria libertà all'interno del mondo elettronico in cui viviamo.

Facciamo un banale esperimento di sopravvivenza informatica, tutti ormai sanno che esiste un controllo del flusso di dati personali e non sulle varie reti che compongono internet, tempo fa avevo già proposto una cosa simile, ma solo come commento su una discussione riguardante la sicurezza e la privacy del singolo utente.

Allora, procediamo per ordine, tutti sanno dell'esistenza di sistemi automatici per il marketing elettronico, ma questi sistemi non hanno solamente questa funzione, la raccolta dei vostri dati, anche se non personali, avviene in ogni momento della vostra vita, con buona pace per chi si è sempre battuto e ha costituito leggi speciali per la tutela della privacy e dei diritti informatici del singolo utente.

La conoscenza specifica dello stile di vita seguito dagli utenti, è molto importante per migliaia di aziende che producono beni utili ed inutili, ma principalmente per i vari governi che possono creare i database relativi ad ogni singola persona per ottenere una mappa globale delle preferenze che possono essere usate poi in modi molto differenti da quelli previsti nell'etica Hacker...

Infatti, seguendo il filone delle e-mail, molti di voi si saranno accorti che dietro ad ogni richiesta, interesse o visita ad un particolare sito web, il browser si popola di strani annunci, ma al momento, non ci pensate perché siete appunto assorti a leggere quello che vi sta interessando in quel preciso istante.

Tempo fa, avevo proposto la storia dei cani e dei gatti per testare sul campo tutti questi sistemi che raccolgono informazioni sulle nostre preferenze e trovare il modo di eluderli per riprenderci la nostra libertà informatica, ecco come procedere:

Il sistema funziona un po in questo modo, l'utente, amante dei cani e dei gatti, ne parla sempre in e-mail con le persone che conosce, avrete capito che l'utente ne parla bene, quindi il sistema di preferenza elettronica registrerà nel suo database che a questo utente, piacciono davvero tanto i cani e i gatti.

A questo punto, l'utente non possiede più la sua libertà, perché riceverà sul proprio browser informazioni mirate per cani e gatti, come e dove comprare il cibo migliore, cure specifiche, etc.etc... :-)))

La contro offensiva da parte dell'utente potrebbe essere impostata in questo modo per eludere i cacciatori di preferenze:

punto 1, l'utente crea due account e-mail, uno per il suo lavoro normale, uno come esca per i sistemi preferenziali automatici.

punto 2, l'utente che decide di riprendersi la propria libertà invia diverse email al secondo account in cui scriverà in modo chiaro e preciso che lui non ama questi animali e che li odia a morte, il sistema si adegua al caso e non invia più pubblicità mirata.

punto 3, l'utente che ama davvero i cani e i gatti, ha semplicemente esposto il suo pensiero elettronico che è stato recepito dal sistema per il controllo elettronico, per cui, l'utente che davvero ama i cani e i gatti, ha raccontato una bugia al sistema per riprendersi il proprio libero arbitrio, è quindi di nuovo libero di scegliere cosa come e dove comprare i prodotti per i suoi animali. :-)

Ma il problema non è davvero ancora risolto per la sopravvivenza in rete, infatti, questi sistemi, tengono in esame non solo il tipo di navigazione fatto dall'utente, ma anche di quanto viene scritto e inviato dalla sua posta elettronica, un banale esempio è che ad un determinato utente arriveranno delle normalissime email pubblicitarie in cui si troveranno diverse informazioni sulle scelte personali che l'utente ha condiviso SOLO tramite i propri contatti personali e non con i siti web che inviano questo tipo di pubblicità.... :-)))

Immagazzinare su un supporto elettronico le vostre esperienze e le

vostre scelte nel corso di tutta la vostra vita, è una cosa non solo fattibile nella realtà, ma questo i vari Governi lo sanno fin troppo bene, non parliamo poi di quando dovrete trovarvi un lavoro, le aziende potranno sapere tutto di voi, e quando dico tutto, intendo proprio questo... :-)

Molte imprese installano programmi per controllare le attività dei propri dipendenti, ma anche se il caso lo richiede, rimane sempre violata l'indipendenza e la libertà dell'utente stesso che è quello che poi dovrà subire tutte le conseguenze del singolo caso.

L'etica Hacker, ci insegna a difendere i principi in cui crediamo, ci insegna a difendere la nostra privacy e ci porta a costruire nuovi programmi per rendere migliore il nuovo mondo elettronico che ci circonda, ci insegna a difendere la nostra libertà e la nostra indipendenza dalle brame dei Governi che vogliono controllarci e sapere sempre tutto di noi e di quello che facciamo in rete.

Cari bloggers, anche per oggi ho lasciato una traccia su questo blog che sarà quindi controllato e studiato da numerosi individui (Governi, Aziende, Tapiri, Smanettoni....;-)))

Come sempre, vi auguro una buona navigazione e un buon divertimento sulle vostre reti preferite, mentre ripensate ai valori dell'etica Hacker esposti oggi in questo breve post... ;-))

Italia di oggi: dove soffia il vento dell'Indipendenza?

Post n°109 pubblicato il **05 Aprile 2014** da exodus1984

Finalmente posso avere un po di tempo per aggiornare il contenuto web e i post di questo blog, cari bloggers, oggi voglio esprimere un mio pensiero personale in merito ad alcuni fatti accaduti di recente che per la loro particolare natura politica, mi hanno spinto a scrivere questo post.

Come tutti ben sapete, l'Italia è ormai un paese stremato da troppe truffe, troppe tasse, troppa inutile burocrazia pagata spremendo i cittadini italiani che ormai, non hanno più nemmeno un lavoro per mantenere un sistema che a molte persone oggi, risulta completamente anti-democratico.

Questo è il risultato di scelte politiche sbagliate, fatte da partiti che dopo essere stati votati, hanno voltato le spalle ai cittadini che li hanno eletti per fare l'interesse della nazione, ma che hanno portato il mio paese, l'Italia, ad una profonda spaccatura tra i già precari rapporti cittadini-stato-politica.

Negli anni, si sono quindi formati gruppi e idee, di carattere politico che seguono la via dell'indipendenza dallo stato italiano, ormai considerato una cosa antica e superata...

Molte delle regioni italiane si sentono ormai "prigioniere" di un sistema-stato che vuole avere tutto, senza mai dare niente in cambio.
Ma andiamo con ordine, perché il sistema-stato italiano viene considerato superato?

Le radici di molti gruppi indipendentisti italiani, si possono ricercare nella scarsa attenzione che il governo italiano ha verso i propri cittadini usando politiche economiche sbagliate che hanno portato la mia povera Italia ad essere quasi un paese da terzo mondo...:-(

Ma le ragioni che spingono molte persone a desiderare l'indipendenza dallo stato italiano, sono ancora più profonde, e molte volte, non hanno nemmeno a che vedere ne con la politica economica del paese, ne con i partiti in causa diretta.

Se le cose non cambieranno in fretta, l'Italia potrebbe ritrovarsi con una guerra civile dovuta appunto alla spaccatura cittadini-stato-politica in cui tutti perderebbero tutto, e nessuno ne uscirebbe vincitore...:-(

L'unità del popolo italiano, è venuta a mancare quando i cittadini italiani hanno provato sulla loro pelle le conseguenze di decisioni politiche sbagliate che hanno portato questo grande paese ad avere un futuro incerto e pericoloso.

Ai politici italiani voglio dire questo:

Fate le scelte giuste per il popolo italiano, e fatele in fretta perché potreste non avere più un'altra occasione per farlo.
Il vento di indipendenza, soffia molto forte, e se non avremo una vera unità nazionale, questa mia povera Italia, sarà davvero perduta per sempre.
Molti gruppi indipendentisti cercano di ottenere solo un riconoscimento della propria terra, delle proprie origini, e penso che in un paese considerato democratico, ognuno possa essere accontentato e soddisfatto per il bene di tutti e per la pace nazionale italiana.

Cerchiamo di costruire insieme un nuovo e grande paese, una nuova Italia che possa tornare ad essere il paese che ho conosciuto un tempo, una

grande nazione rispettata da tutti e considerata di nuovo anche dai governi esteri.

Cari bloggers, oggi ho voluto condividere con tutti voi alcuni pensieri personali che mi stanno assillando da molto tempo, voglio ricordare a tutti che questo non è un blog politico, e non voglio nemmeno che lo diventi solo perché ho espresso il mio pensiero, ma di fronte agli eventi, non potevo non scrivere questo post, ben sapendo che a "qualcuno", non sarebbe stato gradito...

OpenSource: una sfida globale per migliorare il nostro pianeta.

Post n°110 pubblicato il **06 Aprile 2014** da exodus1984
Cari bloggers, oggi con questo veloce post, vorrei informare la comunità degli smanettoni italiani in merito ad un evento che è molto interessante per i progettisti di ingegneria nell'esplorazione spaziale e per il futuro del nostro pianeta, se ancora non ne siete al corrente, leggete qui sotto.

Invio pertanto sul blog un breve estratto dell'invito a questa sfida per il futuro dell'intera umanità.
Potete trovare informazioni/iscrizioni a questo indirizzo web:

https://2014.spaceappschallenge.org/

Questo è un breve estratto per capire subito di cosa si tratta:

International space apps challenge 2014 a Roma 12 e 13 aprile.

75 città coinvolte in 40 sfide su 5 temi:
in arrivo l'hackathon di 48 ore per la risoluzione di problemi posti dall'esplorazione spaziale e per il miglioramento della vita sulla terra.
L'iniziativa è rivolta agli studenti di ingegneria e scienze, ma anche agli appassionati di scienza e spazio di tutto il mondo e avrà luogo simultaneamente in 75 città e 41 paesi in tutto il mondo.

La International Space Apps Challenge ha lo scopo di creare soluzioni opensource ai problemi posti dall'esplorazione spaziale e ai temi legati al miglioramento della vita sulla terra. Durante l'evento si formeranno gruppi di lavoro che avranno accesso a dati pubblici per proporre le loro soluzioni.

Sponsorizzata dalla NASA, organizzata dall'Agenzia Spaziale Europea e dall'Ambasciata degli Stati Uniti in collaborazione con l'Università di Roma La Sapienza, l'International Space Apps Challenge, avrà luogo alla Facoltà di Ingegneria Civile e industriale della Sapienza il 12 e 13 Aprile. Per partecipare basta iscriversi mediante form online.

Detto questo, vi auguro un buon inizio settimana e altrettanti ottimi smanettamenti opensource. :-)))
Buon divertimento a tutti :-)

Sistemi Operativi: Windows e le schermate blu della morte. :-)

Post n°111 pubblicato il **07 Aprile 2014** da exodus1984
Cari bloggers, oggi voglio parlare ancora una volta di sicurezza...;-)
La sicurezza che andremo a vedere oggi, riguarda i sistemi Windows che molti usano per la propria comodità operativa ma che moltissime volte si bloccano lasciando letteralmente "fuori" l'utente autorizzato di questi sistemi, costringendo quest'ultimo, alla formattazione completa del disco fisso.

Qualche post indietro, avevo parlato di un vecchio sistema operativo in grado di risolvere i molti problemi che un utente normale può avere nel corso della vita informatica usando appunto il sistema Windows.

Per prima cosa, voglio raccontarvi come alcune settimane fa, ho riportato in vita un computer portatile che era stato sottoposto a decine e decine di installazioni software, tutte in questo caso dannose e distruttive per il suddetto sistema operativo Windows 7.

Il computer in questione, dopo il suo ultimo "viaggio" su internet, si comportava in un modo alquanto strano, a volte l'utente poteva arrivare fino alla schermata di login, entrando sul sistema prima di venire bloccato dalla cosiddetta "schermata blu della morte", ma molti tentativi di recupero automatico sono andati a vuoto, impedendo in seguito allo sfortunato utente di non arrivare più nemmeno ad usare la modalità provvisoria, ne con grafica limitata, ne in modalità testuale per poter operare a linea di comando, in poche parole, la "modalità sicura" di Windows 7 non era più sicura, perché la schermata blu della morte, aveva preso il sopravvento, impedendo qualunque tentativo di riprendere in mano questa situazione informatica ormai disperata... :-)))

L'utente, disperato non per il sistema operativo, in quanto fornito di backup valido e sicuro, si votava in questo particolare caso alla grazia ricevuta da San RATTO del Friuli, patrono protettore degli utenti disperati sui sistemi Windows... ;-)))

Devo dire che il problema più grande che ho riscontrato durante questa assistenza informatica, è stato il pensiero dell'utente per i file contenuti all'interno del disco, ai quali non si poteva più accedere per via della schermata blu della morte, che arrestava il sistema pochi secondi dopo il boot, impedendo anche alla modalità provvisoria di poter montare un disco esterno su cui scaricare i dati richiesti da questo utente. :-)

Quindi, parlando con l'utente e cercando di capire bene quali file bisognava mettere in salvo, ho preparato un disco esterno usb vuoto su cui poi sarebbero stati riversati i dati richiesti.
Questo disco esterno, è stato poi scansionato da quattro (4) antivirus paralleli su una macchina diversa alla ricerca di virus.

Ma andiamo con ordine, il computer presentava il sospetto di un'infezione grave, per cui la prima cosa utile da fare è stata quella di scaricare un'immagine del sistema RATTO di base, un sistema leggero e veloce, e quindi non modificato, con utility GNU/Linux a livello standard normale, antivirus con un database normale compreso, non modificato:

```
root@exodus84:/home/enrico# fdisk -l

Disk /dev/sda: 1500.3 GB, 1500301910016 bytes
255 heads, 63 sectors/track, 182401 cylinders, total 2930277168 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

```
Disk identifier: 0x000ef6b3

   Device Boot   Start        End     Blocks   Id  System
/dev/sda1   *    2048    48828415    24413184   83  Linux
/dev/sda2    48828416    97656831    24414208   82  Linux swap / Solaris
/dev/sda3    97656832   109375487     5859328   83  Linux
/dev/sda4    109375488  2930276351  1410450432  83  Linux

Disk /dev/sdb: 15.5 GB, 15512174592 bytes
32 heads, 63 sectors/track, 15028 cylinders, total 30297216 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x6cf460fd

   Device Boot      Start        End     Blocks   Id  System
/dev/sdb1            63    30296447    15148192+   b  W95 FAT32

root@exodus84:/home/enrico# dd if=/home/enrico/RATTObaseNOH2004.HDD
of=/dev/sdb bs=512

dd: scrittura di "/dev/sdb": Spazio esaurito sul device
30297217+0 record dentro
30297216+0 record fuori
15512174592 byte (16 GB) copiati, 5275,36 s, 2,9 MB/s

root@exodus84:/home/enrico#
```

Tutti voi sapete che le schermate blu della morte, possono essere imputabili anche ad un malfunzionamento hardware e non solo software. In questo caso, il computer era a posto, perché montando l'immagine d'assalto di RATTO 3.0.2004, il computer funzionava bene senza bloccarsi e permettendomi di montare i dispositivi esterni per il recupero informativo richiesto dall'utente.

Ho fatto una scansione principale parallela sulle quattro(4) partizioni presenti del disco sotto esame, che hanno rivelato la compromissione grave della partizione nascosta di Windows 7, in parole povere, quella che deve essere ripristinata per il corretto riavvio del sistema windows 7.

Quello che ho trovato all'interno di questo supporto, mi ha preoccupato davvero tanto, ma alla fine ho visto che avevo ragione e trovati i file richiesti dall'utente sul suo supporto, ho provveduto a salvarli sul disco esterno.
A questo punto, visto che l'utente disponeva di un backup valido e sicuro ho deciso di ricreare il sistema operativo partendo da questi supporti.

Ma questo piccolo lavoro, impossibile da fare a sentenza di diversi "tecnici", che avendo visto la schermata blu, si ritiravano tutti in buon ordine, consigliando la formattazione del sistema senza nemmeno tentare di salvarlo, come dicevo, questo piccolo lavoro ha portato alla ribalta un sistema che ho costruito per semplificare il mio lavoro e che oggi ha allungato la fila dei credenti Windowsiani che implorano la grazia di San RATTO del Friuli...(Azz... proprio adesso che volevo andarmene in ferie mi arriva tutta questa gente...;-)))

Ritornando a quanto rilevato in assistenza, questo è il risultato:

```
root@warrior:/home/warrior# clamrat -i (su Debian è clamscan -i...:-)

/mnt/c4/avisynth.dll: W32.Heuristic-COC.51.UNOFFICIAL FOUND
/mnt/c4/TCPDeliver.dll: W32.Heuristic-COC.26.UNOFFICIAL FOUND
/mnt/c4/snuninst.exe: W32.Heuristic-COC.62.UNOFFICIAL FOUND
```

/mnt/c4/ISSetup.dll.002: W32.Heuristic-COC.62.UNOFFICIAL FOUND
/mnt/c4/snuninst.exe.003: W32.Heuristic-COC.62.UNOFFICIAL FOUND
/mnt/c4/uninst.exe: W32.MalwareF.IGIL.42.UNOFFICIAL FOUND
/mnt/c4/BackupSetup.exe: TR.Crypt.XPACK.Gen.2183.UNOFFICIAL FOUND
/mnt/c4/lame_enc.dll: W32.Heuristic-COC.6.UNOFFICIAL FOUND
/mnt/c4/StatsReader.exe.001: Generic31.BECJ.2.UNOFFICIAL FOUND
/mnt/c4/DirectShowSource.dll: wgf.heuristic_coc.h.UNOFFICIAL FOUND
/mnt/c4/fmod.dll: W32.Heuristic_COC.7.UNOFFICIAL FOUND
/mnt/c4/ISSetup.dll.003: W32.Heuristic-COC.87.UNOFFICIAL FOUND
/mnt/c4/30355d01: winnow.malware.m0.malware.832426.UNOFFICIAL FOUND
/mnt/c4/AX_UA.dll: Trojan.Click.58277.98.UNOFFICIAL FOUND
/mnt/c4/TurboBoostSetup.exe: W32.Heuristic-COC.87.UNOFFICIAL FOUND
/mnt/c4/mam_ie.exe: TR.Crypt.XPACK.Gen.1214.UNOFFICIAL FOUND
/mnt/c4/Alcohol120_trial_2.0.1.2033.exe: W32.MalwareF.IGIL.42.UNOFFICIAL FOUND
/mnt/c4/snuninst.exe.001: W32.Heuristic-COC.62.UNOFFICIAL FOUND
/mnt/c4/ISSetup.dll.004: W32.Heuristic-COC.62.UNOFFICIAL FOUND
/mnt/c4/StatsReader.exe: Generic31.BECJ.2.UNOFFICIAL FOUND
/mnt/c4/infrarecorder_1210.exe: Adware.W3i.32.10.UNOFFICIAL FOUND
/mnt/c4/snuninst.exe.002: W32.Heuristic-COC.62.UNOFFICIAL FOUND
/mnt/c4/New_Player.exe: TR.Crypt.XPACK.Gen.2183.UNOFFICIAL FOUND
/mnt/c4/ISSetup.dll: W32.Heuristic-COC.62.UNOFFICIAL FOUND
/mnt/c4/ISSetup.dll.001: W32.Heuristic-COC.87.UNOFFICIAL FOUND
/mnt/c4/D57C8d01: winnow.malware.m0.malware.832426.UNOFFICIAL FOUND
/mnt/c4/sp-downloader.exe: wingf.malware_gen.fd.UNOFFICIAL FOUND

---------- SCAN SUMMARY ----------
Known viruses: 3892586
Engine version: 0.97.8
Scanned directories: 1
Scanned files: 28
Infected files: 27
Data scanned: 160.27 MB
Data read: 62.47 MB (ratio 2.57:1)
Time: 48.976 sec (0 m 48 s)

Avendo quindi derattizzato il sistema Windows 7, la schermata blu scompariva, permettendomi di poter provare a recuperare questo sistema però poi risultato instabile, in quanto la schermata blu, ricompariva dopo alcune ore di funzionamento quasi corretto per il sistema compromesso.

Alla fine, ottenuta l'autorizzazione dell'utente per il ripristino via backup e dopo aver portato in salvo i suoi preziosi dati, il portatile era pronto per la sua nuova vita informatica, al riparo da tutti i problemi presentati durante questa breve ma intensa assistenza. ;-)

Cari bloggers, spero che questo piccolo post vi possa servire in qualche modo a comprendere la sicurezza minima che un utente deve sempre avere usando sistemi Windows in modo non adeguato...;-))

Come sempre, un buon proseguimento a tutti sulla rete, e cercate di non prenderveli tutti voi questi virus, lasciatene qualcuno anche a me... ;-)))
Buon divertimento a tutti. ;-)))

25 Aprile: il mistero del RATTO scomparso... ;-)

Post n°112 pubblicato il **25 Aprile 2014** da exodus1984
Cari bloggers, oggi è la festa della Liberazione, e naturalmente anche io mi sono Liberato dai miei impegni...;-)))

Dunque, questo piccolo post è dedicato alle persone che oggi volevano farmi lavorare, ma che non sono riuscite a trovarmi... ;-)))
Premetto che non voglio fuggire dai miei doveri informatici, ma nella giornata di oggi, mi sono reso irreperibile per quasi tutto il giorno.

Questo è un breve estratto del diario di viaggio:

Partenza alle ore 10.30 con destinazione Austria, pranzo in ristorante e successiva destinazione centro commerciale a Villach, con rientro in tarda serata per i consueti spippolamenti informatici... ;-))

Devo dire che la giornata odierna, si è conclusa nel migliore dei modi ma domani mattina mi tocca riprendere in mano la mia vecchia pantegana informatica per tentare di salvare altri dati e sistemi operativi in difficoltà. :-)

Bene bene cari bloggers, adesso vi saluto perché devo preparare il SystemRAT per il lavoro che dovrà svolgere domani, e se la cosa sarà interessante, cercherò di preparare un nuovo post per farvi vedere cosa si riesce a catturare di bello sui computer di certi utenti...;-)

A tutti voi, un buon 25 aprile e un buon fine settimana.

Kernel Linux: un viaggio nel cuore del Pinguino. ;-)

Post n°113 pubblicato il **02 Maggio 2014** da exodus1984
Bene, rieccoci di nuovo qui sul blog a postare i nostri pensieri...;-)

Oggi ho preparato un semplice post che riguarda la compilazione del kernel di Linux, questo post è dedicato alle persone che hanno richiesto questa breve guida, e che non hanno mai provato a ricompilare il nocciolo del proprio sistema GNU/Linux... :-)

Premetto che questa breve guida è fatta solo per le persone che vorrebbero possedere un nuovo kernel sul proprio sistema operativo, ma che comunque non sono dei professionisti o dei tecnici, per cui, se siete smanettoni, oppure dei veri hacker, questa semplice guida non fa per voi... ;-)))
Chiarito questo, possiamo iniziare a vedere i primi passi che un utente non "smanettone" può fare per ottenere e ricompilare un kernel nuovo sul proprio computer Linux.

Per prima cosa, analizzeremo le varie fasi usando un sistema GNU/Linux di default, ovvero la leggendaria distribuzione Debian (www.debian.org). I passi da seguire sono molto semplici, anche se possedete una distro diversa dalla Debian, tutto quello che dovete fare è descritto sempre nelle pagine dei manuali portati dalla distribuzione GNU/Linux che intendete usare, o che usate ogni giorno per lavorare e divertirvi su internet.

A questo punto, dovremo creare una directory di "contenimento" per i nostri kernel, ma anche se intendiamo usarne uno solo, questa dir ci permetterà poi di copiarne il contenuto su un disco esterno e di

trasportare i nostri kernel da una macchina ad un'altra, ma questo passo lo tratteremo più avanti perché ora non ci serve.

Procediamo alla creazione della nostra directory di lavoro:

```
enrico@exodus84:~$ mkdir kernel2013
```

kernel2013 sarà da ora in avanti il vostro parco giochi personale :-)
Naturalmente, potete dargli tutti i nomi che volete voi, ma per questo piccolo esempio, "kernelXXX" va più che bene... ;-))

Listiamo la nostra nuova directory:

```
enrico@exodus84:~$ ls ker*
code.lepus04BSD4.tar  linux-3.12.6          linux-3.14.1.tar.xz
lepus032002.tar       linux-3.12.6.tar.xz   linux-3.14.2
lepus032003.tar       linux-3.12.9.tar.xz   linux-3.14.2.tar.xz
linux-3.11.7          linux-3.12.tar.xz     linux-3.14.tar.xz
linux-3.11.7.tar.xz   linux-3.13.1.tar.xz   RATTO0.1.tar
linux-3.12.2          linux-3.13.2.tar.xz   RATTO2.tar
linux-3.12.2.tar.xz   linux-3.13.5.tar.xz   RATTO3.tar
linux-3.12.3          linux-3.13.6          RATTO4.tar
linux-3.12.3.tar.xz   linux-3.13.6.tar.xz   RATTO5.tar
linux-3.12.4          linux-3.13.7          RATTO6beta.tar
linux-3.12.4.tar.xz   linux-3.13.7.tar.xz   talpix2BSD1999.tar
linux-3.12.5          linux-3.14            talpix3BSD2001.tar
linux-3.12.5.tar.xz   linux-3.14.1          talpix4BSD2002.tar
enrico@exodus84:~/kernel2013$
```

In questo caso, la mia directory è piena di spippoli, ma per voi, questa dir sarà vuota perché adesso andremo a riempirla. :-))

Ora, puntate il vostro browser a questo link:

www.kernel.org

Date un'occhiata agli ultimi kernel definiti stabili, adesso potete scaricare il vostro primo kernel in formato sorgente.
Il kernel che avrete scaricato, andrà depositato nella directory "kernel..." che avete creato in precedenza e dalla quale partirà la

vostra prima compilazione del cuore pulsante di (quasi...) tutte le distribuzioni LinuX. :-)

Bene, entriamo nella nostra directory "kernelXXX", e usando il nostro fidato terminale a linea di comando, impartiamo le prime istruzioni.

Esempio di kernel appena scaricato: linux-3.13.1.tar.xz

xz -d linux-3.13.1.tar.xz

linux-3.13.1.tar

tar xf linux-3.13.1.tar

Se il vostro sistema non dispone dei compressori XZ, andate a questo link per procurarveli: http://tukaani.org/xz/ :-)

Adesso che avete scompattato il vostro primo kernel, sotto la dir "kernelXXX" vi apparirà una nuova directory: linux-3.13.1

entrate quindi all'interno di questa nuova directory:

```
enrico@exodus84:~/kernel2013$ cd linux-3.13.1
enrico@exodus84:~/kernel2013/linux-3.13.1$ ls
arch            Documentation  init     lib         README             sound
block           drivers          ipc      MAINTAINERS  REPORTING-BUGS  tools
COPYING  firmware            Kbuild   Makefile     samples                    usr
CREDITS  fs                      Kconfig  mm          scripts                      virt
crypto          include            kernel   net         security
enrico@exodus84:~/kernel2013/linux-3.13.1$
```

Prepariamo il nostro primo kernel con menuconfig:

```
enrico@exodus84:~/kernel2013/linux-3.13.1$ make menuconfig
[*] 64-bit kernel
|  |      General setup  --->
|  |    [ ] Provide system-wide ring of trusted keys
|  |    [*] Enable loadable module support  --->
|  |    -*- Enable the block layer  --->
|  |      Processor type and features  --->
|  |      Power management and ACPI options  --->
|  |      Bus options (PCI etc.)  --->
|  |      Executable file formats / Emulations  --->
|  |    -*- Networking support  --->

<Select>    < Exit >    < Help >    < Save >    < Load >
```

La prima cosa che potete vedere, è "Processor type and features", per iniziare a preparare il vostro kernel per la macchina specifica su cui poi dovrà operare (per adesso vi basta questo, ma non è tutto quello che vi serve...).

Non scendo nei particolari perché questo post deve risultare semplice per i non addetti ai lavori, per cui, dopo aver verificato il tipo di processore portato dalla vostra macchina, salvate le modifiche e ritornate sul vostro terminale per iniziare la compilazione vera e

propria.

I comandi da usare dopo aver salvato le modifiche al vostro kernel
possono variare di poco:

make   compilazione normale
make -jX compilazione multicore per processori recenti

Date il comando make e premete il tasto invio, se avete una macchina
con cpu multicore, dovete lanciare la compilazione con il comando
make -jX, dove X è il numero di core portato dai processori della
vostra macchina sulla quale compilate il kernel, nel mio caso avremo
un comando make -j8 .

Al termine della compilazione, se tutto è andato per il verso giusto
potrete concludere prima con l'installazione dei moduli prodotti e
poi con l'installazione del vostro nuovo e fimmante kernel.

make modules_install prima installate i moduli creati
make install   poi il resto... :-)

Se tutto è andato bene, riavviate il vostro computer e durante la
fase di boot, leggete se è presente nella lista di Grub il vostro
nuovo kernel, selezionatelo e premete il tasto invio per provare subito
il vostro primo kernel ricompilato da voi stessi. :-)(Kernel_Panic)

Devo dire che come per tutte le cose, anche per il kernel di Linux
potete trovare milioni di FAQ che vi spiegano in modo tecnico o in
modo semplice come ottenere il massimo da una semplice ricompilazione
del codice sorgente, in questo semplice post ho voluto rispondere
ad una richiesta fatta da persone che un kernel non lo avevano mai
installato, benché usino tutti i giorni dei sistemi Linux di varia
natura.

I kernel di installazione delle distribuzioni vanno bene
per essere bootati su un grande numero di macchine con processori
diversi, per questo motivo se si vuole avere più spunto dal proprio
sistema operativo, è bene imparare a ricompilarsi il kernel per le
proprie macchine e per i dispositivi che vogliamo far funzionare
sulla nostra distribuzione GNU/Linux :-)

Potete trovare tutta la documentazione che cercate qui in rete, ma da
buon vecchio lamer, vi consiglio di farvi una vostra esperienza
personale scaricando e ricompilando kernel anche diversi, nel mio
piccolo, di solito riesco a ricompilarne almeno un centinaio all'anno
ma questo valore può variare in base al tipo di sistema che devo
usare, quindi circa 7-9 kernel ogni mese, sempre tenendo conto di
cosa dovrà fare la futura distribuzione creata per ripristinare o
assaltare altri sistemi operativi. :-)

Lo so, lo so, qualcuno di voi sta già pensando che i kernel che riesco
a spippolare in un anno di attività, sono troppo pochi, e che dovrei
darmi da fare di più, ma vi posso dire che per il lavoro che svolgo
sono più che sufficienti e mi danno un sacco di soddisfazioni sia in
rete che a livello di smanettamento personale... ;-)))
Infatti, sul kernel di Linux, ci sono moltissime cose da sapere e da
fare, ma dovrete decidere voi se continuare a ricercare la conoscenza
oppure lasciar fare tutto agli altri... ;-)

Ricompilare il kernel è solo il primo passo, poi avrete voglia di
ricompilare qualche programma, infine potrete arrivare a crearvi un
sistema operativo tutto vostro, e poi... e poi si vedrà... ;-)))
(...se non vi acchiappa prima la Polizia Postale, mentre provate in
rete i vostri ultimi moduli d'assalto appena compilati...:-))).

Spero che questo post risulti abbastanza semplice per gli amici che lo hanno richiesto, ma il mio consiglio è di non fermarvi su questo blog, cercate, leggete e soprattutto smanettate per bene i vostri nuovi kernel, cercate nuove soluzioni, riprogrammate i vostri moduli personali, provate magari a costruire qualcosa di diverso partendo dal kernel Linux. :-) (PanteganiX v.0.0.1XXX ???) ;-)))

Cari amici e cari bloggers, anche per oggi sono riuscito a mandare un post sul blog, ricordandovi di leggere sempre tutta la documentazione dei programmi e delle vostre distribuzioni GNU/Linux, come sempre vi auguro una buona navigazione e un buon divertimento in rete. :-)

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License.